

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001398

International filing date: 01 February 2005 (01.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-125196
Filing date: 21 April 2004 (21.04.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

04. 2. 2005

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 4 月 2 1 日
Date of Application:

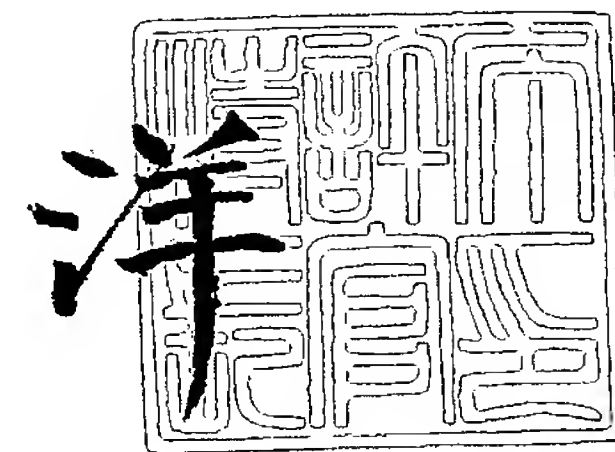
出 願 番 号 特 願 2 0 0 4 - 1 2 5 1 9 6
Application Number:
[ST. 10/C] : [J P 2 0 0 4 - 1 2 5 1 9 6]

出 願 人 松下電器産業株式会社
Applicant(s):

2 0 0 5 年 3 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048160137
【提出日】 平成16年 4月21日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 原田 俊治
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 井藤 好克
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 横田 薫
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 高橋 潤
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】 特許請求の範囲

【請求項 1】

コンテンツを保持する第 1 の装置から第 2 の装置へコンテンツを移動する、もしくは、第 2 の装置から第 1 の装置へコンテンツを移動することが可能な著作権保護システムであつて、

前記第 1 の装置は、第 1 の暗号化コンテンツ、及び、第 1 の暗号化コンテンツと関連する第 2 の暗号化コンテンツを記録するコンテンツ記録部と、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、

前記第 2 の装置は、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを記録するコンテンツ記録部と、前記コンテンツ鍵を記録する鍵記録部とを備え、

前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記第 1 の装置から前記第 2 の装置に移動する際、前記第 1 の装置の鍵制御部による制御の下で、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 2 の装置の鍵記録部に記録し、前記第 1 の装置のコンテンツ記録部に記録している第 1 の暗号化コンテンツ、もしくは、第 2 の暗号化コンテンツを、前記第 2 の装置のコンテンツ記録部に記録することを特徴とする著作権保護システム。

【請求項 2】

前記第 1 の装置の鍵制御部は、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 2 の装置の鍵記録部に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 3】

前記第 1 の装置の鍵制御部は、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 2 の装置の鍵記録部に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 4】

前記第 1 の装置の鍵制御部は、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 2 の装置の鍵記録部に記録し、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を消去することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 5】

前記第 1 の装置は、さらに認証部を備え、前記第 2 の装置は、さらに認証部を備え、前記第 1 の装置の認証部は、前記第 2 の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 2 の装置の鍵記録部に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 6】

前記第 1 の装置は、さらに、認証部、および、鍵暗号部を備え、前記第 2 の装置は、さらに認証部、および、鍵暗号部を備え、

前記第 1 の装置の認証部は、前記第 2 の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第 1 の装置の認証部と、前記第 2 の装置の認証部は、それぞれセッション鍵を生成し、前記第 1 の装置の鍵暗号部は、前記第 1 の装置の鍵記録部に記録しているコンテンツ鍵を前記セッション鍵で暗号化して第 2 の装置に送り、前記第 2 の装置の鍵暗号部は、受け取った暗号化されたコンテンツ鍵を前記セッション鍵で復号し、復号したコンテンツ鍵を前記第 2 の装置の鍵記録部に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 7】

前記第 1 の装置は、さらに、コピー制御情報を記録するコピー制御情報記録部と、前記コピー制御情報に基づいて、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記第 1 の装置から前記第 2 の装置に移動することが認められているか否か

を判定する判定部を備えたことを特徴とする請求項 1 記載の著作権保護システム。

【請求項 8】

前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記第 2 の装置から前記第 1 の装置に移動する際、前記第 1 の装置の鍵制御部による制御の下で、前記第 2 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 1 の装置の鍵記録部に記録し、前記第 2 の装置のコンテンツ記録部に記録している第 1 の暗号化コンテンツ、もしくは、第 2 の暗号化コンテンツを、前記第 1 の装置のコンテンツ記録部に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 9】

前記第 1 の装置の鍵制御部は、前記第 1 の装置の鍵記録部へ記録するコンテンツ鍵を利用不可能な状態にして、前記第 2 の装置の鍵記録部に記録しているコンテンツ鍵を、前記第 1 の装置の鍵記録部に記録し、前記第 2 の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第 1 の装置の鍵記録部へ記録するコンテンツ鍵を利用可能な状態にすることを特徴とする請求項 8 記載の著作権保護システム。

【請求項 10】

コンテンツを、コンテンツ鍵で暗号化したものを第 1 の暗号化コンテンツとし、前記コンテンツを変換して得られた変換コンテンツを、前記コンテンツ鍵で暗号化したものを第 2 の暗号化コンテンツとすることを特徴とする請求項 1 記載の著作権保護システム。

【請求項 11】

前記第 1 の装置が、記録再生装置であり、前記第 2 の装置が、前記記録再生装置により、データの読み書きが可能な可搬媒体であることを特徴とする請求項 1 記載の著作権保護システム。

【請求項 12】

コンテンツを可搬媒体へ移動する、もしくは、可搬媒体からコンテンツを移動することが可能な記録再生装置であって、

第 1 の暗号化コンテンツ、及び、第 1 の暗号化コンテンツと関連する第 2 の暗号化コンテンツを記録するコンテンツ記録部と、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、

前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記記録再生装置から前記可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体に記録し、前記第 1 の装置のコンテンツ記録部に記録している第 1 の暗号化コンテンツ、もしくは、第 2 の暗号化コンテンツを、前記可搬媒体に記録することを特徴とする記録再生装置。

【請求項 13】

前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第 1 の暗号化コンテンツ、もしくは、第 2 の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする請求項 12 記載の記録再生装置。

【請求項 14】

記録再生装置へコンテンツを移動する、もしくは、記録再生装置からコンテンツを移動することが可能な可搬媒体であって、

前記可搬媒体は、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを記録するコンテンツ記録部と、前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部とを備え、

前記第 1 の暗号化コンテンツ、もしくは、前記第 2 の暗号化コンテンツを、前記記録再生装置から可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体の鍵記録部に記録

し、前記記録再生装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記可搬媒体のコンテンツ記録部に記録することを特徴とする可搬媒体。

【請求項15】

前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする請求項14記載の可搬媒体。

【請求項16】

コンテンツを保持する第1の装置から第2の装置へコンテンツを移動する、もしくは、第2の装置から第1の装置へコンテンツを移動することが可能な著作権保護システムであって、

前記第1の装置は、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツを復号するための第1のコンテンツ鍵、及び、前記第2の暗号化コンテンツを復号するための第2コンテンツ鍵を記録する鍵記録部と、前記第1のコンテンツ鍵、及び、第2のコンテンツ鍵へのアクセスを制御する鍵制御部とを備え、

前記第2の装置は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を記録する鍵記録部とを備え、

前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第2の装置のコンテンツ記録部に記録することを特徴とする著作権保護システム。

【請求項17】

前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、並びに、第2のコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録した第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第1の装置の鍵記録部から消去することを特徴とする請求項16記載の著作権保護システム。

【請求項18】

前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第2の装置から前記第1の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第1の装置のコンテンツ記録部に記録することを特徴とする請求項16記載の著作権保護システム。

【請求項19】

前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を利用不可能な状態にして、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を消去し、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を利用可能な状態にすることを特徴とする請求項18記載の著作権保護システム。

【書類名】 明細書

【発明の名称】 記録再生装置、可搬媒体、及び著作権保護システム

【技術分野】

【0001】

本発明は、コンテンツの不正利用防止を目的とした記録再生装置、及び可搬媒体を含む著作権保護システムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。

【背景技術】

【0002】

近年、BSデジタル放送や地上デジタル放送の開始に伴い、映画等のデジタルコンテンツが広く配信されるようになってきている。デジタルコンテンツ（以下、コンテンツ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツを保護）するための技術開発が進められている。

【0003】

このようなコンテンツの保護技術に関する規格として、例えば、DTCP (Digital Transmission Content Protection) がある。DTCPは、コンテンツをデジタル転送する際に、コンテンツを暗号化するなどして不正コピーを防止する技術である。DTCPのようなコンテンツ保護技術においては、コンテンツに、「Copy No More」、「Copy One Generation」等のコピー制御情報 (CCI: Copy Control Information) を付与する。「Copy No More」はコンテンツのコピーが禁止されていることを表し、「Copy One Generation」はコンテンツのコピーが1回だけ許されていることを表す。従って、コピー制御情報として「Copy One Generation」が付与されたコンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報として「Copy No More」が付与される。

【0004】

一方で、コピー制御情報として「Copy No More」が付与されたコンテンツであっても、他の記録媒体、あるいは他の装置へ移動させたいという要望がある。例えば、デジタルテレビに内蔵されているHDD (Hard Disk Drive) に記録されているコンテンツをDVD-RAMに移動させて保存版として保管しておきたいような場合である。この際 (HDDからDVD-RAMにコンテンツを移動させた場合)、デジタルテレビ内蔵HDDの当該コンテンツは、当然、再生できない状態にされなければならない。例えば、内蔵HDDからDVD-RAMにコンテンツをコピーした後に、内蔵HDDに記録されているコンテンツを消去するなどしてコンテンツを無効化する、すなわちコンテンツを利用できない状態にする方法などが考えられる。しかしながら、コンテンツの移動に先立ってデジタルテレビから内蔵HDDを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、コンテンツを移動した後にバックアップしておいたデータを内蔵HDDに戻すという操作が行われると、コンテンツを何度でも移動できることになり、事実上不正コピーを防止することができなくなる。

【0005】

また、内蔵のHDDからDVD-RAMにコンテンツをコピーした後、内蔵HDDに記録されているコンテンツを消去する方法では、コピーした後に、記録再生装置から記録媒体を不正に引き抜かれた場合に、記録再生装置の内蔵HDDと、DVD-RAMの両方にコンテンツが存在し、不正コピーを防止できなくなる。

【0006】

また、コンテンツの移動中の電源断などの原因により、移動元と移動先のコンテンツが共に損なわれ、コンテンツとして利用できなくなることは、コンテンツを利用するユーザにとっては不便である。さらに、このようにして利用できなくなったコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。

【0007】

上記課題を解決するための従来技術として、不正コピーを防止しながら、コンテンツの喪失を招くことなく、コンテンツの移動を可能にする技術が特許文献1に開示されている。

【特許文献1】特開2003-228522号公報

【非特許文献1】「現代暗号理論」、池野信一、小山謙二、電子通信学会

【非特許文献2】「暗号理論入門」、岡本栄司、共立出版株式会社

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、移動元のコンテンツが高画質コンテンツであり、コンテンツのサイズに比べて、移動先の記録容量が小さい場合には、コンテンツの移動前に、その画質を劣化させるなどしてサイズを小さく圧縮変換してから移動を行うのが通例であるが、前記構成のようにコンテンツを消去するなどして移動元のコンテンツを無効化する場合、圧縮変換された（画質の劣化した）コンテンツだけがユーザの下に残ることになる。すなわち、再び記録容量の大きな内蔵HDDへコンテンツを戻す（移動する）場合であっても、画質の劣化されたコンテンツを高画質コンテンツへ変換することは不可能であり、元々の高画質コンテンツは復元されないため、これはコンテンツを利用するユーザの利便性が損なわれることにつながる。

【0009】

本発明は、前記課題を解決するものであって、不正コピーを防止しながら、コンテンツの喪失を招くことなくコンテンツの移動を可能にして、さらに、サイズを小さくする圧縮の変換後であっても、当該コンテンツを移動元に戻す場合には、元々の高画質コンテンツの復元を可能にする記録再生装置、並びに可搬媒体を含む著作権保護システムの提供を目的とする。

【課題を解決するための手段】

【0010】

本発明は、コンテンツを保持する第1の装置から第2の装置へコンテンツを移動する、もしくは、第2の装置から第1の装置へコンテンツを移動することが可能な著作権保護システムであって、前記第1の装置は、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第2の装置は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記コンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第2の装置のコンテンツ記録部に記録することを特徴とする。

【0011】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録することを特徴とする。

【0012】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録することを特徴とする。

【0013】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を消去することを特徴とする。

【0014】

また、前記第1の装置は、さらに認証部を備え、前記第2の装置は、さらに認証部を備え、前記第1の装置の認証部は、前記第2の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を、前記第2の装置の鍵記録部に記録することを特徴とする。

【0015】

また、前記第1の装置は、さらに、認証部、および、鍵暗号部を備え、前記第2の装置は、さらに認証部、および、鍵暗号部を備え、前記第1の装置の認証部は、前記第2の装置の認証部との間で認証処理を行い、認証処理が成功したときに、前記第1の装置の認証部と、前記第2の装置の認証部は、それぞれ、セッション鍵を生成し、前記第1の装置の鍵暗号部は、前記第1の装置の鍵記録部に記録しているコンテンツ鍵を前記セッション鍵で暗号化して第2の装置に送り、前記第2の装置の鍵暗号部は、受け取った暗号化されたコンテンツ鍵を前記セッション鍵で復号し、復号したコンテンツ鍵を前記第2の装置の鍵記録部に記録することを特徴とする。

【0016】

また、前記第1の装置は、さらに、コピー制御情報を記録するコピー制御情報記録部と、前記コピー制御情報に基づいて、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動することが認められているか否かを判定する判定部を備えたことを特徴とする。

【0017】

また、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第2の装置から前記第1の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第1の装置のコンテンツ記録部に記録することを特徴とする。

【0018】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部へ記録するコンテンツ鍵を利用不可能な状態にして、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録しているコンテンツ鍵を消去し、前記第1の装置の鍵記録部へ記録するコンテンツ鍵を利用可能な状態にすることを特徴とする。

【0019】

また、コンテンツを、コンテンツ鍵で暗号化したものを第1の暗号化コンテンツとし、前記コンテンツを変換して得られた変換コンテンツを、前記コンテンツ鍵で暗号化したものを第2の暗号化コンテンツとすることを特徴とする。

【0020】

また、前記第1の装置が、記録再生装置であり、前記第2の装置が、前記記録再生装置により、データの読み書きが可能な可搬媒体であることを特徴とする。

【0021】

また、コンテンツを可搬媒体へ移動する、もしくは、可搬媒体からコンテンツを移動することが可能な記録再生装置であって、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部と、前記コンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記記録再生

装置から前記可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記可搬媒体に記録することを特徴とする。

【0022】

また、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする。

【0023】

また、記録再生装置へコンテンツを移動する、もしくは、記録再生装置からコンテンツを移動することが可能な可搬媒体であって、前記可搬媒体は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを復号するためのコンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記記録再生装置から可搬媒体に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記記録再生装置の鍵記録部に記録しているコンテンツ鍵を、前記可搬媒体の鍵記録部に記録し、前記記録再生装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記可搬媒体のコンテンツ記録部に記録することを特徴とする。

【0024】

また、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記可搬媒体から前記記録再生装置に移動する際、前記記録再生装置の鍵制御部による制御の下で、前記可搬媒体の鍵記録部に記録しているコンテンツ鍵を、前記記録再生装置の鍵記録部に記録し、前記可搬媒体のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記記録再生装置のコンテンツ記録部に記録することを特徴とする。

【0025】

また、コンテンツを保持する第1の装置から第2の装置へコンテンツを移動する、もしくは、第2の装置から第1の装置へコンテンツを移動することが可能な著作権保護システムであって、前記第1の装置は、第1の暗号化コンテンツ、及び、第1の暗号化コンテンツと関連する第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1の暗号化コンテンツを復号するための第1のコンテンツ鍵、及び、前記第2の暗号化コンテンツを復号するための第2コンテンツ鍵を記録する鍵記録部と、前記第1のコンテンツ鍵、及び、第2のコンテンツ鍵へのアクセスを制御する鍵制御部とを備え、前記第2の装置は、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを記録するコンテンツ記録部と、前記第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を記録する鍵記録部とを備え、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第1の装置から前記第2の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第1の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第2の装置のコンテンツ記録部に記録することを特徴とする。

【0026】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、並びに、第2のコンテンツ鍵を利用不可能な状態にして、前記第1の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第2の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録した第1のコンテンツ鍵

、もしくは、第2のコンテンツ鍵を、前記第1の装置の鍵記録部から消去することを特徴とする。

【0027】

また、前記第1の暗号化コンテンツ、もしくは、前記第2の暗号化コンテンツを、前記第2の装置から前記第1の装置に移動する際、前記第1の装置の鍵制御部による制御の下で、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置のコンテンツ記録部に記録している第1の暗号化コンテンツ、もしくは、第2の暗号化コンテンツを、前記第1の装置のコンテンツ記録部に記録することを特徴とする。

【0028】

また、前記第1の装置の鍵制御部は、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を利用不可能な状態にして、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは、第2のコンテンツ鍵を、前記第1の装置の鍵記録部に記録し、前記第2の装置の鍵記録部に記録している第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を消去し、前記第1の装置の鍵記録部へ記録する第1のコンテンツ鍵、もしくは第2のコンテンツ鍵を利用可能な状態にすることを特徴とする。

【発明の効果】

【0029】

本発明によれば、移動処理の実行により、オリジナルの高画質コンテンツが失われることがなく、また、移動処理時に、コンテンツの圧縮変換処理や暗号化処理が不要なため、高速に移動処理が行えるという効果を有する。

【発明を実施するための最良の形態】

【0030】

以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置101と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置102と、前記移動するコンテンツを獲得する記録再生装置103、あるいは可搬媒体104からなる。

【0031】

記録再生装置102は、コンテンツ供給装置101からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵HDDに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認（認証）した上で、コンテンツの移動を実行する。さらに、記録再生装置102は、コンテンツの移動が完了した後に、内部に記録するコンテンツを利用できない状態にする。ここで、認証技術は、例えば、相手が装置であれば、DTCP規格で定められた手順を用いることができ、相手が可搬媒体であればCPRM SD (Content Protection for Recordable Media Specification SD Memory Card Book) 規格で定められた手順を用いることができる。あるいは、非特許文献1、並びに非特許文献2に開示される公知の任意の技術を用いることができる。このように認証技術は、公知の技術で実現可能なため、その詳細についてはここでは言及しない。

【0032】

（実施の形態1）

図2は、本発明の実施の形態1における、記録再生装置102がコンテンツを記録、並びに再生を行い、さらに記録再生装置102から可搬媒体104にコンテンツを移動させる場合の記録再生装置102、並びに可搬媒体104の機能を示す機能ブロック図である。

【0033】

記録再生装置102は、外部からコピー制御情報と、コンテンツを受信する受信部20

1 と、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置 102（具体的には、後述する暗号化コンテンツ記録部 210、211）に記録することが認められているか否かを判定する判定部 202 と、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部 204 と、前記受信したコンテンツを暗号化するために用いるコンテンツ鍵を生成する鍵生成部 205 と、前記生成したコンテンツ鍵を記録するコンテンツ鍵記録部 206 と、コンテンツ鍵記録部 206 に記録したコンテンツ鍵へのアクセスを制御する制御部 203 と、前記コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第 1 暗号化コンテンツを生成する暗号化部 208 と、前記第 1 暗号化コンテンツを記録する暗号化コンテンツ記録部 210 と、前記受信したコンテンツを、変換する変換部 207 と、前記コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第 2 暗号化コンテンツを生成する暗号化部 209 と、前記第 2 暗号化コンテンツを記録する暗号化コンテンツ記録部 211 とを備える。

【0034】

また、記録再生装置 102 は、さらに、前記第 1 暗号化コンテンツ、もしくは、第 2 暗号化コンテンツを、前記コンテンツ鍵を用いて復号化する復号化部 221 と、復号した第 1 暗号化コンテンツ、もしくは、復号した第 2 暗号化コンテンツを再生する再生部 222 と、コピー制御情報記録部 204 に記録したコピー制御情報に基づいて、暗号化コンテンツ記録部 211 に記録した第 2 暗号化コンテンツを、記録再生装置 102 から可搬媒体 104 に移動することが認められているか否かを判定する、もしくは、後述する可搬媒体 104 のコピー制御情報記録部 216 に記録したコピー制御情報に基づいて、可搬媒体 104 の暗号化コンテンツ記録部 218 に記録した第 2 暗号化コンテンツを、可搬媒体 104 から記録再生装置 102 に移動することが認められているか否かを判定する判定部 212 と記録再生装置 102 と可搬媒体 104 との間で、相互に、相手が正当であるか否かを認証する認証部 223、認証が成功した時に、記録再生装置 102 と可搬媒体 104 との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部 225、コピー制御情報記録部 204 に記録したコピー制御情報、コンテンツ鍵記録部 206 に記録したコンテンツ鍵、並びに、暗号化コンテンツ記録部 211 に記録した第 2 暗号化コンテンツを可搬媒体 104 に書き込む、もしくは、可搬媒体 104 から読み出す書込／読出部 213 とを備える。

【0035】

記録再生装置 102 が備える制御部 203、コピー制御情報記録部 204、並びに、コンテンツ鍵記録部 206 は、外部からのデータの読み書きが不可能なセキュアな領域 214 に設けられる。この領域 214 は、具体的には、耐タンパハードウェア、耐タンパソフトウェア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部 210、211 は、外部からの読み書きが可能な領域 215 に設けられる。この領域 215 は、例えば、HDD（Hard Disk Drive）により構成する。

【0036】

一方、可搬媒体 104 は、記録再生装置 102 と可搬媒体 104 との間で、相互に、相手が正当であるか否かを認証する認証部 224 と、認証が成功した時に、記録再生装置 102 と可搬媒体 104 との間で、やり取りされるコンテンツ鍵、及び、コピー制御情報を暗号化、復号化するための暗号化／復号化部 226 とを備える。

【0037】

また、可搬媒体 104 は、さらに、前記第 2 暗号化コンテンツを記録する暗号化コンテンツ記録部 218 と、前記コンテンツ鍵を記録するコンテンツ鍵記録部 217 と、前記コピー制御情報を記録するコピー制御情報記録部 216 を備える。可搬媒体 104 が備えるコピー制御情報記録部 216、並びに、コンテンツ鍵記録部 217 は、外部から正当な装置以外読み書きできない領域 219 に設けられる。この領域 219 は、可搬媒体 104 の認証部 224 と、記録再生装置 102 の認証部 223 との間で、認証処理が正しく実行できた場合のみ、記録再生装置 102 からのデータの読み書きが可能となる領域である。暗号化コンテンツ記録部 218 は、外部からの読み書きが可能な領域 220 に設けられる。

【0038】

次に、図3を用いて、受信したコンテンツを記録再生装置102に記録する場合の動作について説明する。

【0039】

S301：記録再生装置102の受信部201は、コンテンツとコピー制御情報を受信する。

【0040】

S302：判定部202は、「前記コピー制御情報が、受信したコンテンツを記録再生装置102に記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「記録は認められる」と判定した場合は、以降の処理を実行する。

【0041】

S303：前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部204に記録する。

【0042】

S304：鍵生成部205は、コンテンツ鍵を生成し、コンテンツ鍵記録部206に記録する。

【0043】

S305：暗号化部208は、受信したコンテンツを、コンテンツ鍵記録部206に記録しているコンテンツ鍵で暗号化して第1暗号化コンテンツを生成する。

【0044】

S306：前記第1暗号化コンテンツを暗号化コンテンツ記録部210に記録する。

【0045】

S307：変換部207は、受信したコンテンツを、変換する。

【0046】

S308：暗号化部209は、前記変換したコンテンツを、コンテンツ鍵記録部206に記録しているコンテンツ鍵で暗号化して第2暗号化コンテンツを生成する。

【0047】

S309：前記第2暗号化コンテンツを暗号化コンテンツ記録部211に記録する。

【0048】

ここで、コピー制御情報としては、例えば、コピーが禁止されていることを示す「Copy Never」や、コピーが1回だけ許されていることを示す「Copy One Generation」などが用いられる。この場合、判定部202は、コピー制御情報が「Copy Never」であれば、「記録は認められない」と判定し、コピー制御情報が「Copy One Generation」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記録再生装置に記録するのに伴い、コピー制御情報は、「Copy One Generation」から、コピー禁止を示す「No More Copy」へ更新してコピー制御情報記録部204に記録する。

【0049】

変換部207は、例えば、受信したコンテンツが、MP EG 2形式の映像コンテンツである場合に、MP EG 4形式の映像コンテンツに変換する。

【0050】

次に、図4を用いて、記録再生装置102から、可搬媒体104へコンテンツを移動する場合の動作について説明する。

【0051】

S401：記録再生装置102の判定部212は、書込／読出部213を介して、コピー制御情報記録部204に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部211に記録した第2暗号化コンテンツを可搬媒体104に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

められる」と判定した場合は、以降の処理を実行する。

【0052】

S402:記録再生装置104の認証部223は、可搬媒体104の認証部224との間で相互認証を行い、相互認証が成功した時は、認証部223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【0053】

S403:書込/読出部213は、コピー制御情報記録部204に記録しているコピー制御情報、並びに、コンテンツ鍵記録部206に記録しているコンテンツ鍵を読み出す。

【0054】

このとき、制御部203は、コンテンツ鍵記録部206に記録しているコンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

【0055】

S404:書込/読出部213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化/復号化部225にて、前記セッション鍵を用いて暗号化して可搬媒体104に送り、可搬媒体104は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化/復号化部226にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体104に記録する。

【0056】

S405:コピー制御情報記録部204に記録しているコピー制御情報と、コンテンツ鍵記録部206に記録しているコンテンツ鍵を消去する。

【0057】

S406:書込/読出部213は、暗号化コンテンツ記録部211に記録している第2暗号化コンテンツを読み出す。

【0058】

S407:読み出した第2暗号化コンテンツを可搬媒体104に記録する。

【0059】

S408:暗号化コンテンツ記録部211に記録している第2暗号化コンテンツを消去する。

【0060】

図5、図6は、上記動作における記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。図5(a)は、上記ステップS401の開始時点、(b)は、上記ステップS403の終了時点、(c)は、ステップS404の終了時点、(d)は、ステップS405の終了時点、図6(e)は、ステップS407の終了時点、(f)は、ステップS408の終了時点である。

【0061】

ここで、ステップS403において、制御部203は、コンテンツ鍵記録部206に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップS404が終了し、ステップS405が開始する前のタイミングで(図5(c))、電源断、もしくは、可搬媒体104を記録再生装置102から不正に引き抜く事などが行われたとしても、記録再生装置102と、可搬媒体104の両方において同時にコンテンツ鍵が利用可能な状態で存在することを防止できる。また、図5(a)～図6(f)のどのタイミングで電源断が起こっても、記録再生装置102と、可搬媒体104のいずれかにおいてコンテンツ鍵は存在するため、移動元と移動先の両方でコンテンツ鍵が共に損なわれコンテンツが利用できなくなることはない。

【0062】

ステップS402における認証部223、224で実行される相互認証、及び、セッション鍵共有方法としては、例えば、チャレンジャーレスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジャーレスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

【0063】

次に、図7を用いて、可搬媒体104から、記録再生装置102へコンテンツを移動する場合の動作について説明する。

【0064】

S601：記録再生装置102の判定部212は、書込／読出部213を介して、可搬媒体104のコピー制御情報記録部216に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、可搬媒体104の暗号化コンテンツ記録部218に記録した第2暗号化コンテンツを記録再生装置102に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【0065】

S602：記録再生装置104の認証部223は、可搬媒体104の認証部224との間で相互認証を行い、相互認証が成功した時は、認証部223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【0066】

S603：書込／読出部213は、可搬媒体104のコピー制御情報記録部216に記録しているコピー制御情報、並びに、コンテンツ鍵記録部217に記録しているコンテンツ鍵を読み出す。このとき、可搬媒体104の暗号化／復号化部226にて、コピー制御情報、並びに、コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置102に送り、記録再生装置102の暗号化／復号化部225は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部213に送る。

【0067】

S604：書込／読出部213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、記録再生装置102のコピー制御情報記録部204、並びに、コンテンツ鍵記録部206にそれぞれ記録する。このとき、制御部223は、コンテンツ鍵記録部206に記録したコンテンツ鍵はアクセスできないよう利用不可状態にする。

【0068】

S605：可搬媒体104のコピー制御情報記録部216に記録しているコピー制御情報、並びに、コンテンツ鍵記録部217に記録しているコンテンツ鍵を消去する。

【0069】

制御部223は、コンテンツ鍵記録部206に記録したコンテンツ鍵がアクセスできるように利用可能状態にする。

【0070】

S606：書込／読出部213は、可搬媒体104の暗号化コンテンツ記録部218に記録している第2暗号化コンテンツを読み出す。

【0071】

S607：読み出した第2暗号化コンテンツを記録再生装置102の暗号化コンテンツ記録部211に記録する。

【0072】

S608：可搬媒体104の暗号化コンテンツ記録部218に記録している第2暗号化コンテンツを消去する。

【0073】

図8、図9は、上記動作における記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。図8(a)は、上記ステップS601の開始時点、(b)は、上記ステップS604の終了時点、(c)は、ステップS605の終了時点、(d)は、ステップS607の終了時点、図9(e)は、ステップS608の終了時点である。

【0074】

次に、図10を用いて、記録再生装置102において、記録した第1暗号化コンテンツ

、もしくは、第2暗号化コンテンツを再生する場合の動作について説明する。

【0075】

S801：復号化部221は、暗号化コンテンツ記録部210、もしくは、暗号化コンテンツ記録部211より、第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを読み出す。

【0076】

S802：復号化部221は、コンテンツ鍵記録部206より、コンテンツ鍵を読み出す。

【0077】

このとき、制御部203は、コンテンツ鍵記録部206に記録しているコンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

【0078】

S803：復号化部221は、読み出した第1暗号化コンテンツ、もしくは、第2暗号化コンテンツを、読み出したコンテンツ鍵を用いて復号化する。

【0079】

S804：再生部222は、復号した第1暗号化コンテンツもしくは、第2暗号化コンテンツを再生する。再生が終了すると、コンテンツ鍵記録部206に記録しているコンテンツ鍵を利用可能状態にする。

【0080】

ここで、ステップS802において、制御部203により、コンテンツ鍵はアクセスできない利用不可状態にされるので、第1暗号化コンテンツの復号及び再生処理と、第2暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

【0081】

(変形例)

実施の形態1では、第2暗号化コンテンツが記録再生装置102から可搬媒体104に移動する場合において、記録再生装置102の制御部203が、コンテンツ鍵を読み出されたときアクセスできないように利用不可状態にしたが、この構成を変えて、可搬媒体104の領域219に制御部を設けても良い。この場合、第2暗号化コンテンツが記録再生装置102から可搬媒体104に移動する場合の動作は次の通りである。

【0082】

T401：記録再生装置102の判定部212は、書込／読出部213を介して、コピー制御情報記録部204に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部211に記録した第2暗号化コンテンツを可搬媒体104に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【0083】

T402：記録再生装置104の認証部223は、可搬媒体104の認証部224との間で相互認証を行い、相互認証が成功した時は、認証部223、224はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【0084】

T403：書込／読出部213は、コピー制御情報記録部204に記録しているコピー制御情報、並びに、コンテンツ鍵記録部206に記録しているコンテンツ鍵を読み出す。

【0085】

T404：書込／読出部213は、読み出したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部225にて、前記セッション鍵を用いて暗号化して可搬媒体104に送り、可搬媒体104は、受け取った暗号化したコピー制御情報、並びに、コンテンツ鍵を、暗号化／復号化部226にて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、コンテンツ鍵を可搬媒体104に記録する。

【0086】

このとき、可搬媒体の制御部は、可搬媒体 104 のコンテンツ鍵記録部 217 に記録しているコンテンツ鍵が、アクセスできないように利用不可状態にする。

【0087】

T405: コピー制御情報記録部 204 に記録しているコピー制御情報、並びに、コンテンツ鍵記録部 206 に記録しているコンテンツ鍵を消去する。

【0088】

このとき、可搬媒体 104 の制御部は、コンテンツ鍵記録部 217 に記録しているコンテンツ鍵が、アクセスできるように利用可能状態にする。

【0089】

T406: 書込/読出部 213 は、暗号化コンテンツ記録部 211 に記録している第 2 暗号化コンテンツを読出す。

【0090】

T407: 読み出した第 2 暗号化コンテンツを可搬媒体 104 に記録する。

【0091】

T408: 暗号化コンテンツ記録部 211 に記録している第 2 暗号化コンテンツを消去する。

【0092】

同様に、実施の形態 1 では、第 2 暗号化コンテンツが可搬媒体 104 から記録再生装置 102 に移動する場合において、記録再生装置 102 の制御部 203 が、コンテンツ鍵が読み出されたときアクセスできないように利用不可状態にしたが、この構成に変えて、可搬媒体 104 の領域 219 に制御部を設けても良い。この場合の動作については、上記ステップ T401 から T408 と同様であるので説明は省略する。

【0093】

また、実施の形態 1 では、記録再生装置 102 に制御部 203 を設ける構成としたが、記録再生装置 102 と、可搬媒体 104 の双方に、制御部を設ける構成としてもよい。

【0094】

以上、本発明の実施の形態 1 では、受信したコンテンツと、それを変換したコンテンツとを、それぞれ、同一のコンテンツ鍵を用いて、暗号化する構成について説明したが、この構成に限定されない。すなわち、受信したコンテンツと、それを変換したコンテンツとを、異なるコンテンツ鍵を用いて、暗号化する構成としてもよい。この場合について、以下、実施の形態 2 として説明する。

【0095】

(実施の形態 2)

図 11 は、本発明の実施の形態 2 における、記録再生装置 102a がコンテンツを記録、並びに再生を行い、さらに記録再生装置 102a から可搬媒体 104a にコンテンツを移動させる場合の記録再生装置 102a、並びに可搬媒体 104a の機能を示す機能ブロック図である。

【0096】

記録再生装置 102a は、外部からコピー制御情報と、コンテンツを受信する受信部 201a と、前記コピー制御情報に基づき、前記受信したコンテンツを記録再生装置 102a (具体的には、後述する暗号化コンテンツ記録部 210a、211a) に記録することが認められているか否かを判定する判定部 202a と、前記コピー制御情報を、必要に応じて更新した後、記録するコピー制御情報記録部 204a と、前記受信したコンテンツを暗号化するために用いる第 1 コンテンツ鍵と、第 2 コンテンツ鍵を生成する鍵生成部 205a と、前記生成した第 1 コンテンツ鍵を記録するコンテンツ鍵記録部 206a1 と、前記生成した第 2 コンテンツ鍵を記録するコンテンツ鍵記録部 206a2 と、コンテンツ鍵記録部 206a1、206a2 に記録された第 1 コンテンツ鍵、第 2 コンテンツ鍵へのアクセスを制御する制御部 203a と、前記第 1 コンテンツ鍵を用いて、前記受信したコンテンツを暗号化して、第 1 暗号化コンテンツを生成する暗号化部 208a と、前記第 1 暗号化コンテンツを記録する暗号化コンテンツ記録部 210a と、前記受信したコンテンツ

を、変換する変換部 207a と、前記第 2 コンテンツ鍵を用いて、前記変換したコンテンツを暗号化して第 2 暗号化コンテンツを生成する暗号化部 209a とを備える。

【0097】

また、記録再生装置 102a は、さらに、前記第 2 暗号化コンテンツを記録する暗号化コンテンツ記録部 211a と、前記第 1 暗号化コンテンツ、もしくは、第 2 暗号化コンテンツを、前記第 1 コンテンツ鍵、もしくは、前記第 2 コンテンツ鍵を用いて復号化する復号化部 221a と、復号した第 1 暗号化コンテンツ、もしくは、復号した第 2 暗号化コンテンツを再生する再生部 222a と、コピー制御情報記録部 204a に記録したコピー制御情報に基づいて、暗号化コンテンツ記録部 211a に記録した第 2 暗号化コンテンツを、記録再生装置 102a から可搬媒体 104a に移動することが認められているか否か判定する、もしくは、後述する可搬媒体 104a のコピー制御情報記録部 216a に記録したコピー制御情報に基づいて、可搬媒体 104a の暗号化コンテンツ記録部 218a に記録した第 2 暗号化コンテンツを、可搬媒体 104a から記録再生装置 102a に移動することが認められているか否か判定する判定部 212a と、記録再生装置 102a と可搬媒体 104a との間で、相互に、相手が正当であるか否かを認証する認証部 223a、認証部 224a と、認証が成功した時に、記録再生装置 102a と可搬媒体 104a との間で、やりとりされるコピー制御情報、並びに、第 1 コンテンツ鍵、もしくは、第 2 コンテンツ鍵を暗号化、復号化するための暗号化／復号化部 225a、226a と、コピー制御情報記録部 204a に記録したコピー制御情報と、コンテンツ鍵記録部 206a1 に記録した第 1 コンテンツ鍵、もしくは、コンテンツ鍵記録部 206a2 に記録した第 2 コンテンツ鍵と、並びに、暗号化コンテンツ記録部 211a に記録した第 2 暗号化コンテンツを可搬媒体 104a に書込む、もしくは、可搬媒体 104a から読み出す書込／読出部 213a とを備える。

【0098】

記録再生装置が備えるコピー制御情報記録部 204a、制御部 203a、並びに、コンテンツ鍵記録部 206a1、206a2 は、外部からのデータの読み書きが不可能なセキュアな領域 214a に設けられる。この領域 214a は、具体的には、耐タンパハードウェア、耐タンパソフトウェア、あるいは、両者の組み合わせで構成する。暗号化コンテンツ記録部 210a、211a は、外部からの読み書きが可能な領域 215a に設けられる。この領域 215a は、例えば、HDD (Hard Disk Drive) により構成する。

【0099】

一方、可搬媒体 104a は、記録再生装置 102a と可搬媒体 104a との間で、相互に、相手が正当であるか否かを認証する認証部 224a と、認証が成功した時に、記録再生装置 102a と可搬媒体 104a との間で、やりとりされるコピー制御情報、並びに、第 1 コンテンツ鍵、もしくは、第 2 コンテンツ鍵を暗号化、復号化するための暗号化／復号化部 226a とを備える。

【0100】

また、可搬媒体 104a は、さらに、前記第 2 暗号化コンテンツを記録する暗号化コンテンツ記録部 218a と、前記第 1 コンテンツ鍵、もしくは、第 2 コンテンツ鍵を記録するコンテンツ鍵記録部 217a と、前記コピー制御情報を記録するコピー制御情報記録部 216a を備える。可搬媒体 104a が備えるコピー制御情報記録部 216a、並びに、前記コンテンツ鍵記録部 217a は、外部から正当な装置以外読み書きできない領域 219a に設けられる。この領域 219a は、可搬媒体 104a の認証部 224a と、記録再生装置の認証部 223a との間で、認証処理が正しく実行できた場合のみ、前記記録再生装置 102a からのデータの読み書き可能となる領域である。暗号化コンテンツ記録部 218a は、外部からの読み書きが可能な領域 220a に設けられる。

【0101】

次に、図 12 を用いて、受信したコンテンツを記録再生装置 102a に記録する場合の動作について説明する。

【0102】

S301a：記録再生装置102aの受信部201aは、コンテンツとコピー制御情報を受信する。

【0103】

S302a：判定部202aは、「前記コピー制御情報が、受信したコンテンツを記録再生装置102aに記録することが認められているか否か」を判定する。判定の結果、「記録は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「記録は認められる」と判定した場合は、以降の処理を実行する。

【0104】

S303a：前記コピー制御情報を、必要に応じて更新してコピー制御情報記録部204aに記録する。

【0105】

S304a：鍵生成部205aは、第1コンテンツ鍵、および、第2コンテンツ鍵を生成し、それぞれコンテンツ鍵記録部206a1、206a2に記録する。

【0106】

S305a：暗号化部208aは、受信したコンテンツを、コンテンツ鍵記録部206a1に記録している第1コンテンツ鍵で暗号化して第1暗号化コンテンツを生成する。

【0107】

S306a：前記第1暗号化コンテンツを暗号化コンテンツ記録部210aに記録する。

【0108】

S307a：変換部207aは、受信したコンテンツを、変換する。

【0109】

S308a：暗号化部209aは、前記変換したコンテンツを、コンテンツ鍵記録部206a2に記録している第2コンテンツ鍵で暗号化して第2暗号化コンテンツを生成する。

【0110】

S309a：前記第2暗号化コンテンツを暗号化コンテンツ記録部211aに記録する。

【0111】

ここで、コピー制御情報としては、実施の形態1の場合と同様に、例えば、コピーが禁止されていることを示す「Copy Never」や、コピーが1回だけ許されていることを示す「Copy One Generation」などが用いられる。この場合、判定部202aは、コピー制御情報が「Copy Never」であれば、「記録は認められない」と判定し、コピー制御情報が「Copy One Generation」であれば、「記録は認められている」と判定する。後者の場合、コンテンツを記録再生装置に記録するのに伴い、コピー制御情報は、「Copy One Generation」から、これ以上コピー禁止を示す「No More Copy」へ更新してコピー制御情報記録部204aに記録する。

【0112】

変換部207aは、例えば、受信したコンテンツが、MPEG2形式の映像コンテンツである場合に、MPEG4形式の映像コンテンツに圧縮変換する。

【0113】

次に、図13を用いて、記録再生装置102aから、可搬媒体104aへコンテンツを移動する場合の動作について説明する。

【0114】

S401a：記録再生装置102aの判定部212aは、書込／読出部213aを介して、コピー制御情報記録部204aに記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、暗号化コンテンツ記録部211aに記録した第2暗号化コンテンツを可搬媒体104aに移動することが認められているか否か」を判定する。判定の結果

果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【0115】

S402a: 記録再生装置104aの認証部223aは、可搬媒体104aの認証部224aとの間で相互認証を行い、相互認証が成功した時は、認証部223a、224aはそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【0116】

S403a: 書込/読出部213aは、コピー制御情報記録部204aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部206a2に記録している第2コンテンツ鍵を読み出す。

【0117】

このとき、制御部203aは、コンテンツ鍵記録部206a1に記録している第1コンテンツ鍵および、コンテンツ鍵記録部206a2に記録している第2コンテンツ鍵が、以降、アクセスできないように利用不可状態にする。

【0118】

S404a: 書込/読出部213aは、読み出したコピー制御情報、並びに、第2コンテンツ鍵を、暗号化/復号化部225aにて、前記セッション鍵を用いて暗号化して可搬媒体104aに送り、可搬媒体104aは、受け取った暗号化したコピー制御情報、並びに、第2コンテンツ鍵を、暗号化/復号化部226aにて、前記セッション鍵を用いて復号し、復号したコピー制御情報、並びに、第2コンテンツ鍵を可搬媒体104aに記録する。

【0119】

S405a: コピー制御情報記録部204aに記録しているコピー制御情報、並びに、コンテンツ鍵記録部206a2に記録している第2コンテンツ鍵を消去する。

【0120】

S406a: 書込/読出部213aは、暗号化コンテンツ記録部211aに記録している第2暗号化コンテンツを読み出す。

【0121】

S407a: 読み出した第2暗号化コンテンツを可搬媒体104aに記録する。

【0122】

S408a: 暗号化コンテンツ記録部211aに記録している第2暗号化コンテンツを消去する。

【0123】

図14、図15は、上記動作における記録再生装置102a、並びに可搬媒体104aにおける各データの記録状態を示した図である。図14(a)は、上記ステップS401aの開始時点、(b)は、上記ステップS403aの終了時点、(c)は、ステップS404aの終了時点、(d)は、ステップS405aの終了時点、図15(e)は、ステップS407aの終了時点、(f)は、ステップS408aの終了時点である。

【0124】

ここでステップS403aにおいて、制御部203aは、コンテンツ鍵記録部206a1に記録している第1コンテンツ鍵、及び、コンテンツ鍵記録部206a2に記録している第2コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。これにより、ステップS404aが終了し、ステップS405aが開始する前のタイミングで、電源断、もしくは、可搬媒体104aを記録再生装置102aから不正に引き抜く事などが行われたとしても、記録再生装置102aと、可搬媒体104aの両方において同時に、第1コンテンツ鍵と第2コンテンツ鍵が利用可能な状態で存在することを防止できる。また、図14(a)～図15(f)のどのタイミングで電源断が起こっても、記録再生装置102aと、可搬媒体104aのいずれかにおいて第1コンテンツ鍵、及び、第2コンテンツ鍵は存在するため、移動元と移動先の両方で、第1コンテンツ鍵、及び、第2コンテンツ

鍵が共に損なわれコンテンツが利用できなくなることはない。

【0 1 2 5】

ステップ S 4 0 2 a における認証部 2 2 3 a、2 2 4 a で実行される相互認証、及び、セッション鍵共有方法としては、実施の形態 1 と同様に、例えば、チャレンジレスポンス型の相互認証、セッション鍵共有方法を用いる。チャレンジレスポンス型の相互認証、セッション鍵共有方法については、公知であるので説明は省略する。

【0 1 2 6】

次に、図 1 6 を用いて、可搬媒体 1 0 4 a から、記録再生装置 1 0 2 a へコンテンツを移動する場合の動作について説明する。

【0 1 2 7】

S 6 0 1 a：記録再生装置 1 0 2 a の判定部 2 1 2 a は、書込／読出部 2 1 3 a を介して、可搬媒体 1 0 4 a のコピー制御情報記録部 2 1 6 a に記録されているコピー制御情報を受け取り、「受け取ったコピー制御情報が、可搬媒体 1 0 4 a の暗号化コンテンツ記録部 2 1 8 a に記録した第 2 暗号化コンテンツを記録再生装置 1 0 2 a に移動することが認められているか否か」を判定する。判定の結果、「移動は認められない」と判定した場合は、以降の処理を中止し終了する。判定の結果、「移動は認められる」と判定した場合は、以降の処理を実行する。

【0 1 2 8】

S 6 0 2 a：記録再生装置 1 0 4 a の認証部 2 2 3 a は、可搬媒体 1 0 4 a の認証部 2 2 4 a との間で相互認証を行い、相互認証が成功した時は、認証部 2 2 3 a、2 2 4 a はそれぞれセッション鍵を生成する。前記相互認証処理が失敗した時は、以降の処理を中止し終了する。

【0 1 2 9】

S 6 0 3 a：書込／読出部 2 1 3 a は、可搬媒体 1 0 4 a のコピー制御情報記録部 2 1 6 a に記録しているコピー制御情報、並びに、コンテンツ鍵記録部 2 1 7 a に記録している第 2 コンテンツ鍵を読み出す。このとき、可搬媒体 1 0 4 a の暗号化／復号化部 2 2 6 a にて、コピー制御情報、並びに、第 2 コンテンツ鍵は、前記セッション鍵を用いて暗号化して、記録再生装置 1 0 2 a に送り、記録再生装置 1 0 2 a の暗号化／復号化部 2 2 5 a は、受け取った暗号化したコピー制御情報、並びに、第 2 コンテンツ鍵を、前記セッション鍵を用いて復号して、書込／読出部 2 1 3 a に送る。

【0 1 3 0】

S 6 0 4 a：書込／読出部 2 1 3 a は、読み出したコピー制御情報、並びに、第 2 コンテンツ鍵を、記録再生装置 1 0 2 a のコピー制御情報記録部 2 0 4 a、並びに、コンテンツ鍵記録部 2 0 6 a 2 にそれぞれ記録する。このとき、制御部 2 0 3 a は、コンテンツ鍵記録部 2 0 6 a 2 に記録した第 2 コンテンツ鍵はアクセスできないよう利用不可状態にする。

【0 1 3 1】

S 6 0 5 a：可搬媒体 1 0 4 a のコピー制御情報記録部 2 1 6 a に記録しているコピー制御情報、並びに、コンテンツ鍵記録部 2 1 7 a に記録している第 2 コンテンツ鍵を消去する。

【0 1 3 2】

制御部 2 0 3 a は、コンテンツ鍵記録部 2 0 6 a 2 に記録したコンテンツ鍵、並びに、コンテンツ鍵記録部 2 0 6 a 1 に記録した第 1 コンテンツ鍵を利用可能状態にする。

【0 1 3 3】

S 6 0 6 a：書込／読出部 2 1 3 a は、可搬媒体 1 0 4 a の暗号化コンテンツ記録部 2 1 8 a に記録している第 2 暗号化コンテンツを読み出す。

【0 1 3 4】

S 6 0 7 a：読み出した第 2 暗号化コンテンツを記録再生装置 1 0 2 a の暗号化コンテンツ記録部 2 1 1 a に記録する。

【0 1 3 5】

S 608 a: 可搬媒体 104 a の暗号化コンテンツ記録部 218 a に記録している第 2 暗号化コンテンツを消去する。

【0136】

図 17、図 18 は、上記動作における記録再生装置 102 a、並びに可搬媒体 104 a における各データの記録状態を示した図である。図 17 (a) は、上記ステップ S 601 a の開始時点、(b) は、上記ステップ S 604 a の終了時点、(c) は、ステップ S 605 a の終了時点、(d) は、ステップ S 607 a の終了時点、図 18 (e) は、ステップ S 608 a の終了時点である。

【0137】

次に、図 19 を用いて、記録再生装置 102 a において、記録した第 1 暗号化コンテンツ、もしくは、第 2 暗号化コンテンツを再生する場合の動作について説明する。

【0138】

S 701 a: 復号化部 221 a は、暗号化コンテンツ記録部 210 a、もしくは、暗号化コンテンツ記録部 211 a より、第 1 暗号化コンテンツ、もしくは、第 2 暗号化コンテンツを読み出す。

【0139】

S 702 a: 復号化部 221 a は、コンテンツ鍵記録部 206 a 1 より第 1 コンテンツ鍵を、もしくは、コンテンツ鍵記録部 206 a 2 より第 2 コンテンツ鍵を読み出す。

【0140】

このとき、制御部 203 a は、コンテンツ鍵記録部 206 a 1 に記録している第 1 コンテンツ鍵、及び、コンテンツ鍵記録部 206 a 2 に記録している第 2 コンテンツ鍵が、以降、アクセスできないよう利用不可状態にする。

【0141】

S 703 a: 復号化部 221 a は、読み出した第 1 暗号化コンテンツ、もしくは、第 2 暗号化コンテンツを、読み出した第 1 コンテンツ鍵、もしくは、第 2 コンテンツ鍵を用いて復号化する。

【0142】

S 704 a: 再生部 222 a は、復号した第 1 暗号化コンテンツもしくは、第 2 暗号化コンテンツを再生する。

【0143】

ここで、ステップ S 702 a において、制御部 203 a により、第 1 コンテンツ鍵、もしくは、第 2 コンテンツ鍵はアクセスできないよう利用不可状態にされるので、第 1 暗号化コンテンツの復号及び再生処理と、第 2 暗号化コンテンツの復号及び再生処理は、排他的にしか実行できない。

【0144】

(その他の変形例)

(1) 上記実施の形態 1、及び上記実施の形態 2 において、コンテンツ供給装置 101、101 a から記録再生装置 102、102 a へのコンテンツの供給方法としては、地上波、あるいは、衛星などを介した放送、インターネットなどを介した通信、DVD などの記録メディアを介した方法など、さまざまな方法が利用できる。

【0145】

(2) 上記実施の形態 1、及び上記実施の形態 2 において、受信部 201、201 a にて、受信したコンテンツや、コピー制御情報は、暗号化されていてもよい。この場合は、判定部 202、202 a で処理する前に、暗号化されたコンテンツやコピー制御情報は復号化するものとする。

【0146】

(3) 上記実施の形態 1、及び上記実施の形態 2 では、受信したコンテンツから、1つの変換したコンテンツを作成し、暗号化して記録する構成を説明したが、この構成に限定されない。例えば、受信したコンテンツから、複数の異なる変換を施したコンテンツを作成し、暗号化して記録し、そのうちの一つないし複数の記録再生装置から可搬媒体に移動

するように構成してもよい。また実施の形態1、及び実施の形態2では、受信したコンテンツ自身は変換しない構成としたが、受信したコンテンツ自身を、(第2暗号化コンテンツとは異なる形式で)変換したものであるとしてもよい。

【0147】

(4) 上記実施の形態1、及び上記実施の形態2では、記録再生装置102、102aの鍵生成部205、205aにて、コンテンツ鍵、第1コンテンツ鍵、第2コンテンツ鍵を生成し、コンテンツ鍵記録部206、206a1、206a2に記録するものとしたが、この構成に限定されない。例えば、コンテンツ鍵は、外部で生成され、記録再生装置102、102aに供給される構成としてもよい。

【0148】

(5) 上記実施の形態1、及び上記実施の形態2において、可搬媒体104、104aとしては、例えば、SDメモリカードを用いることができる。この場合、認証部223、224、223a、224a、及び、暗号化/復号化部225、226、225a、226aは、CPRM SD規格により決められた方式に従って実行する。

【0149】

(6) 上記実施の形態1、及び上記実施の形態2では、第2暗号化コンテンツを、記録再生装置102、102aから可搬媒体104、104aに移動する場合について説明したが、第1暗号化コンテンツを記録再生装置102、102aから可搬媒体104、104aに移動するとしてもよい。

【0150】

(7) 上記実施の形態1、及び上記実施の形態2では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

【0151】

(8) このとき、例えば、記録再生装置102、及び、記録再生装置103の認証部、及び、暗号化/復号化部は、DTCF規格により決められた方式に従って実行する。

【0152】

(9) 上記実施の形態1、及び上記実施の形態2では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する際、記録再生装置、並びに可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必要なコンテンツ鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。また、データの消去ではなく、データを不正にアクセスできない利用不可能状態にする構成であってもよい。

【0153】

(10) 上記実施の形態1、及び上記実施の形態2において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初からやり直すかを決定する構成であってもよい。

【0154】

(11) 上記実施の形態1、及び上記実施の形態2において、記録再生装置、並びに可搬媒体が、コンテンツ鍵を移動後に消去する場合、コンテンツ鍵の受信側が、コンテンツ鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信

を確認した後に、コンテンツ鍵を消去する構成であってもよい。

【0 1 5 5】

(1 2) 上記実施の形態 1、及び上記実施の形態 2 において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

【0 1 5 6】

(1 3) 上記実施の形態 1、及び上記実施の形態 2 において、複数のコンテンツに対する、第 1 暗号化コンテンツ、第 2 暗号化コンテンツをそれぞれ作成し、暗号化コンテンツ記録部 2 1 0、2 1 1、2 1 0 a、2 1 1 a に記録し、複数のコンテンツに対する、コピー制御情報、並びに、コンテンツ鍵（もしくは、第 1 コンテンツ鍵、第 2 コンテンツ鍵）を、それぞれコピー制御情報記録部 2 0 4、2 0 4 a、コンテンツ鍵記録部 2 0 6、2 0 6 a 1、2 0 6 a 2 に記録する構成としてもよい。この場合、コンテンツと、それに対応するコンテンツ鍵、並びに、コピー制御情報が分かるように、例えば、コンテンツ識別情報を、第 1 暗号化コンテンツ、及び、第 2 暗号化コンテンツを、暗号化コンテンツ記録部 2 1 0、2 1 1、2 1 0 a、2 1 1 a に記録するときに一緒に記録し、また、コピー制御情報、並びに、コンテンツ鍵（もしくは、第 1 コンテンツ鍵、第 2 コンテンツ鍵）を、それぞれ、コピー制御情報記録部 2 0 4、2 0 4 a、並びに、コンテンツ鍵記録部 2 0 6、2 0 6 a 1、2 0 6 a 2 に記録するときに、前記コンテンツ識別情報を一緒に記録する構成としてもよい。これにより、例えば、ある第 2 暗号化コンテンツを可搬媒体 1 0 4 a に移動するとき、そのコンテンツ識別情報と同じコンテンツ識別情報を有するコピー制御情報、並びにコンテンツ鍵（もしくは、第 1 コンテンツ鍵、第 2 コンテンツ鍵）を、コピー制御情報記録部 2 0 4、2 0 4 a、並びに、コンテンツ鍵記録部 2 0 6、2 0 6 a 1、2 0 6 a 2 より見出すことが可能となる。

【0 1 5 7】

(1 4) 上記実施の形態 1、及び上記実施の形態 2 では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

【産業上の利用可能性】

【0 1 5 8】

本発明にかかる著作権保護システムは、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツを復号するための鍵も合わせて移動させることにより、記録再生装置内のコンテンツを消去することなく利用不可状態にすることができ、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記復号するための鍵を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にできるという効果を有し、ユーザ利便性を損なわない著作権保護システムの実現において有用である。

【図面の簡単な説明】

【0 1 5 9】

【図 1】 本発明に係る著作権保護システムの全体構成を示すブロック図

【図 2】 本発明の実施の形態 1 における機能ブロック図

【図 3】 本発明の実施の形態 1 における記録再生装置にコンテンツを記録する際の動作フロー図

【図 4】 本発明の実施の形態 1 における記録再生装置から可搬媒体へコンテンツを移

動させる際の動作フロー図

【図 5】本発明の実施の形態 1 における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図 6】本発明の実施の形態 1 における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図 7】本発明の実施の形態 1 における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図

【図 8】本発明の実施の形態 1 における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図 9】本発明の実施の形態 1 における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図 10】本発明の実施の形態 1 における記録再生装置に記録したコンテンツを再生する際の動作フロー図

【図 11】本発明の実施の形態 1 における機能ブロック図

【図 12】本発明の実施の形態 2 における記録再生装置にコンテンツを記録する際の動作フロー図

【図 13】本発明の実施の形態 2 における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー図

【図 14】本発明の実施の形態 2 における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図 15】本発明の実施の形態 2 における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図 16】本発明の実施の形態 2 における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー図

【図 17】本発明の実施の形態 2 における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図 18】本発明の実施の形態 2 における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図 19】本発明の実施の形態 2 における記録再生装置に記録したコンテンツを再生する際の動作フロー図

【符号の説明】

【0160】

101 コンテンツ供給装置

102, 102a 記録再生装置

103 記録再生装置

104, 104a 可搬媒体

201, 201a 受信部

202, 202a 判定部

203, 203a 制御部

204, 204a, 216, 216a コピー制御情報記録部

205, 205a 鍵生成部

206, 206a1, 206a2, 217, 217a コンテンツ鍵記録部

207, 207a 変換部

208, 208a, 209, 209a 暗号化部

210, 210a, 211, 211a, 218, 218a 暗号化コンテンツ記録部

212, 212a 判定部

213, 213a 書込／読出部

214, 214a, 215, 215a, 219, 219a, 220, 220a 領域

221, 221a 復号化部

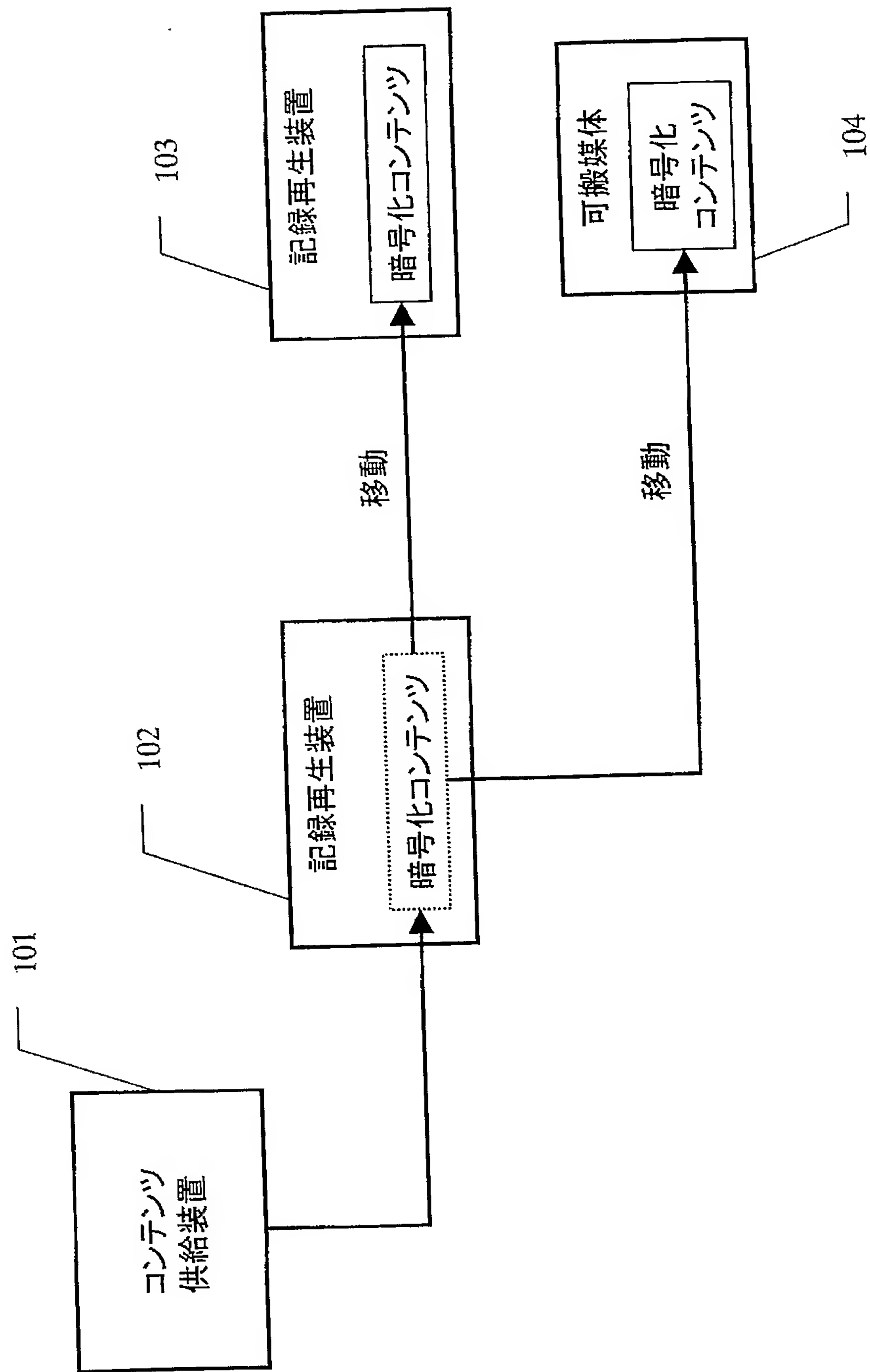
222, 222a 再生部

2 2 3, 2 2 3 a, 2 2 4, 2 2 4 a
2 2 5, 2 2 5 a, 2 2 6, 2 2 6 a

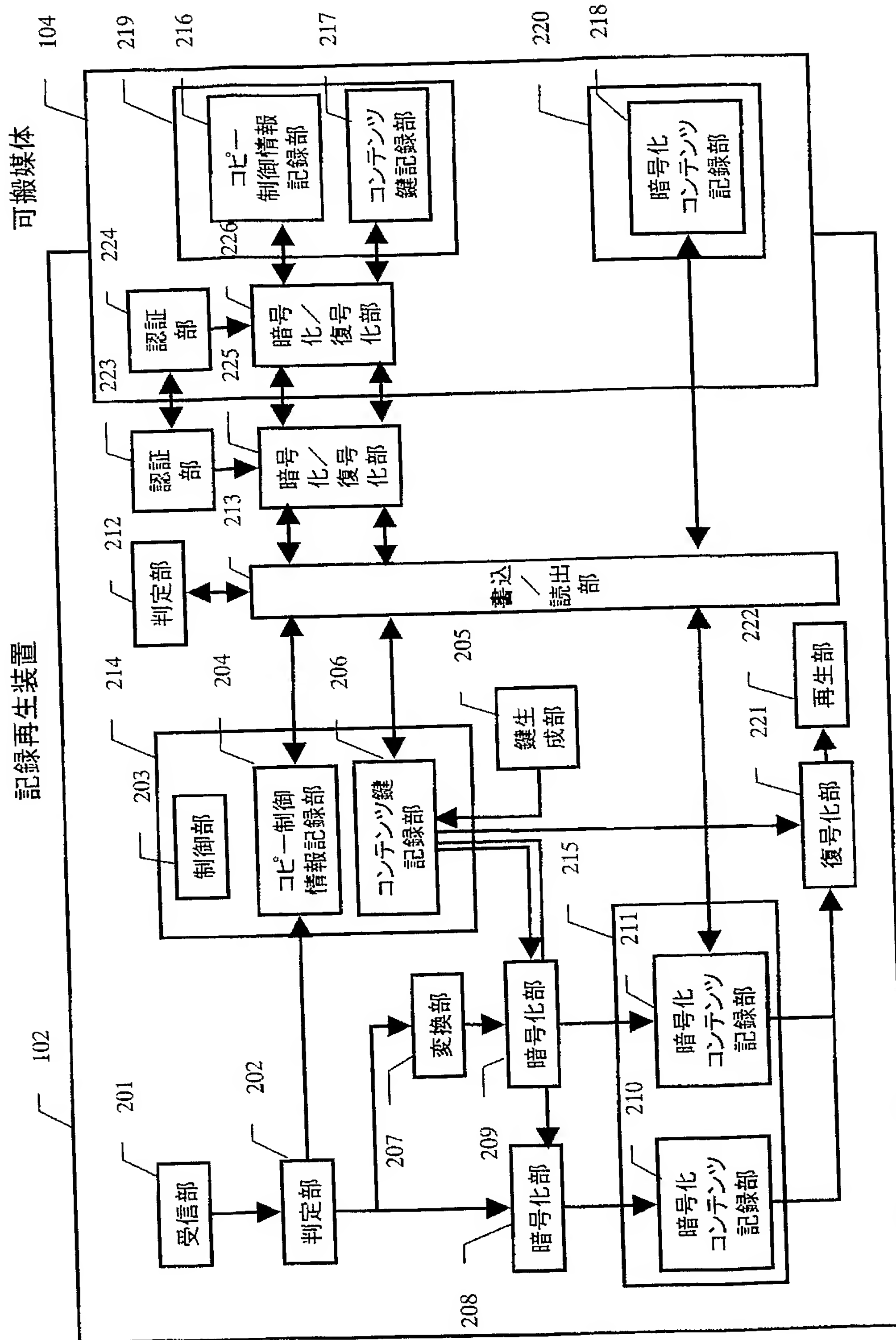
認証部
暗号化／復号化部

【書類名】 図面

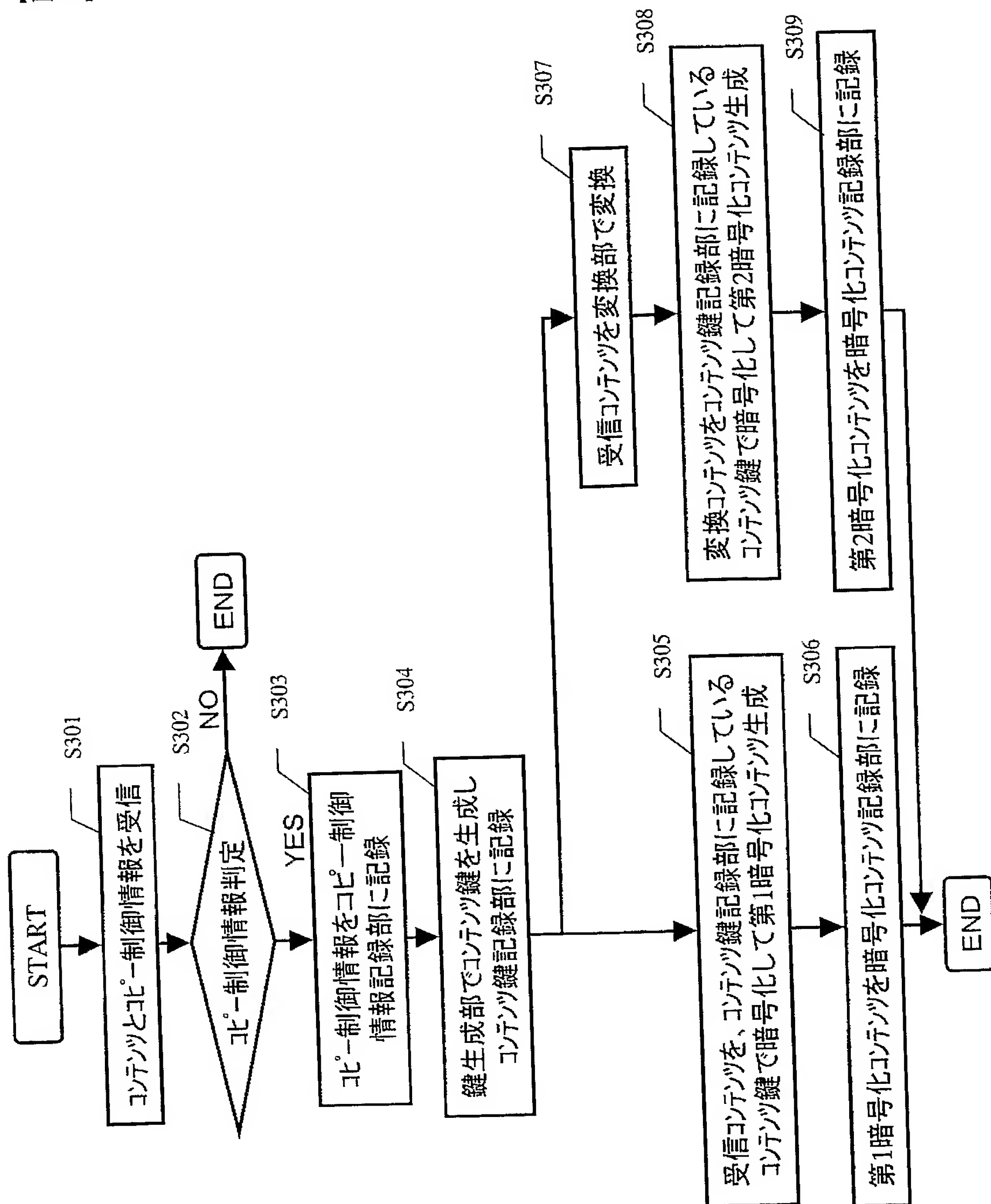
【図 1】



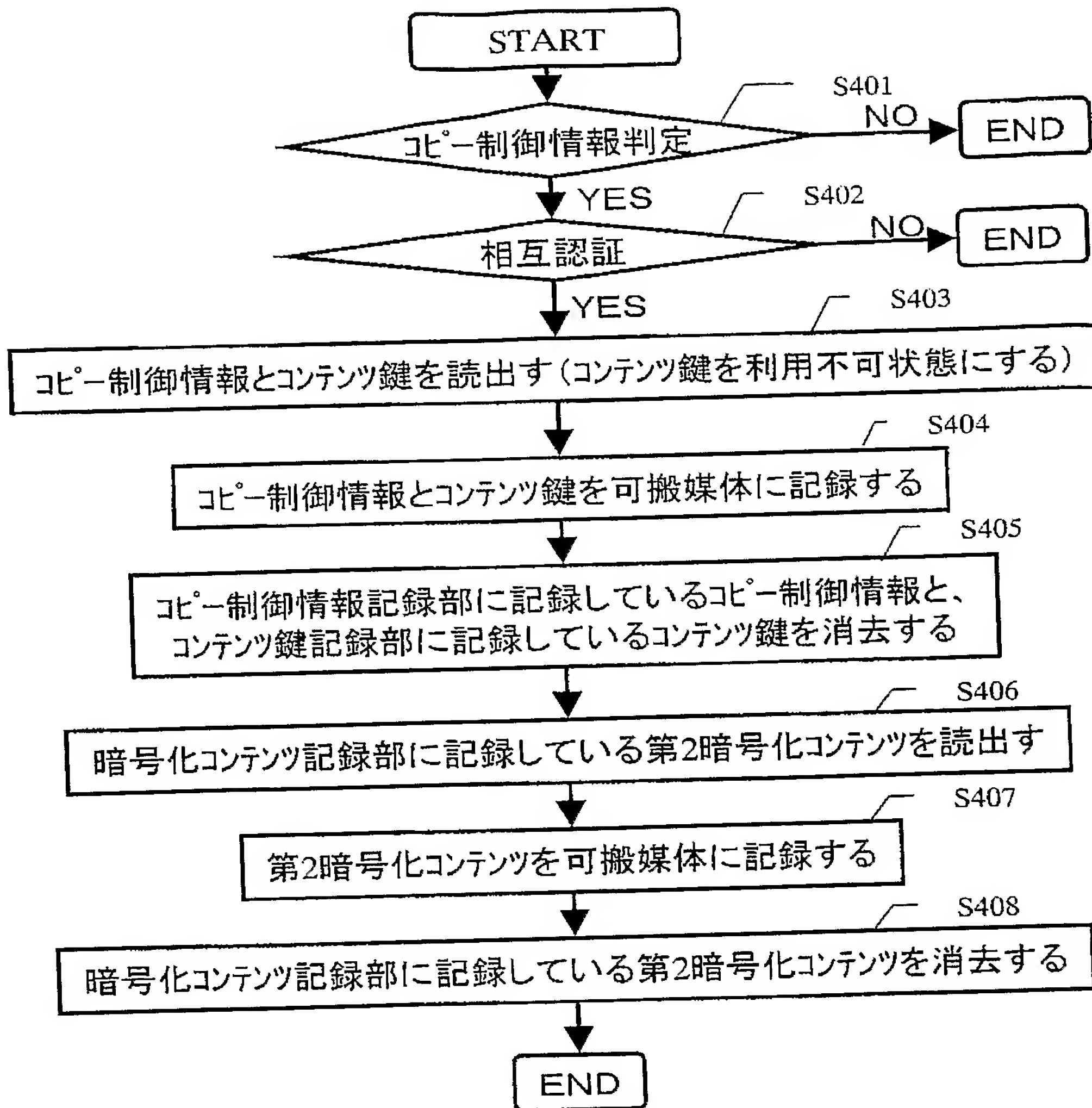
【図 2】



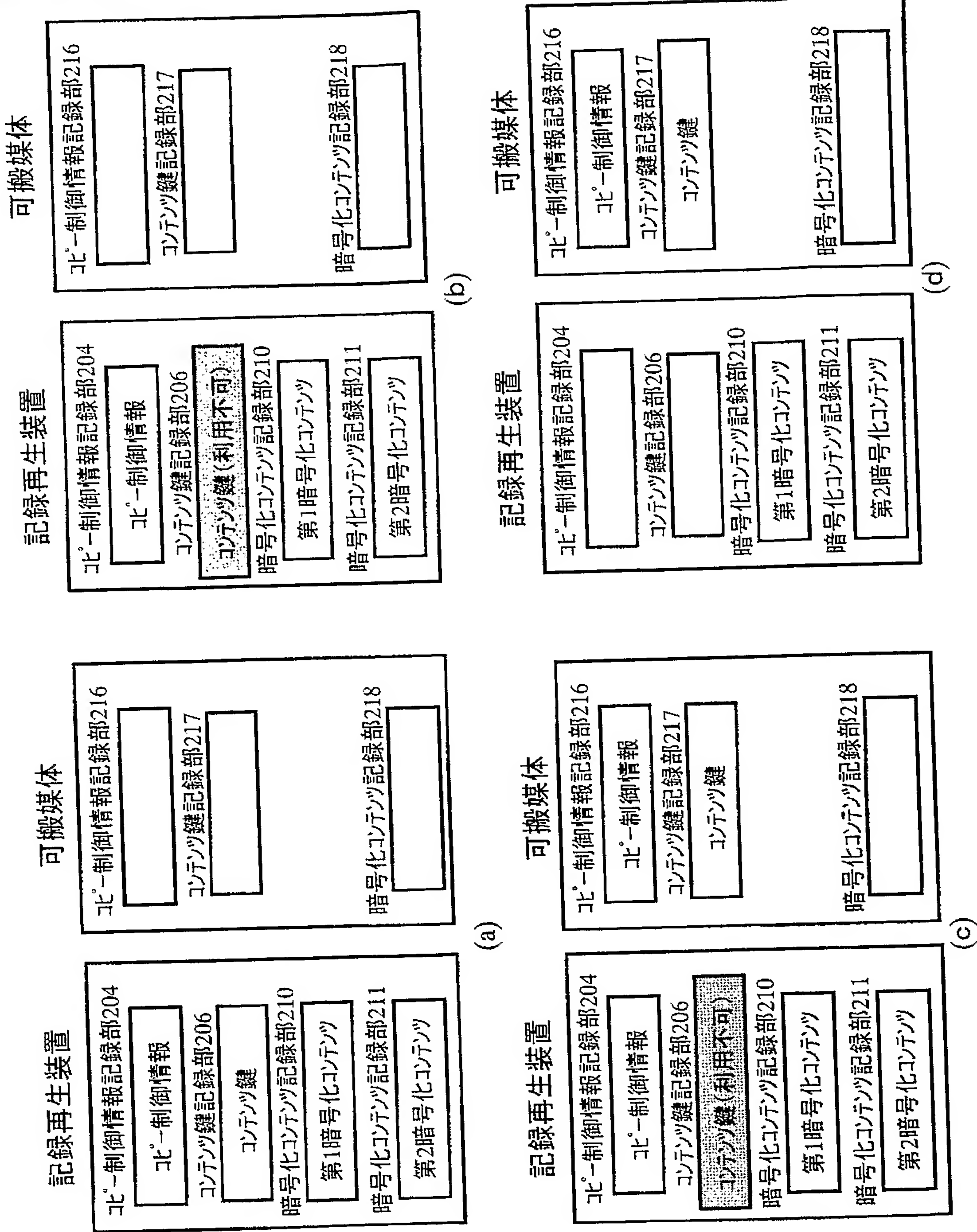
【図 3】



【図 4】



【図 5】



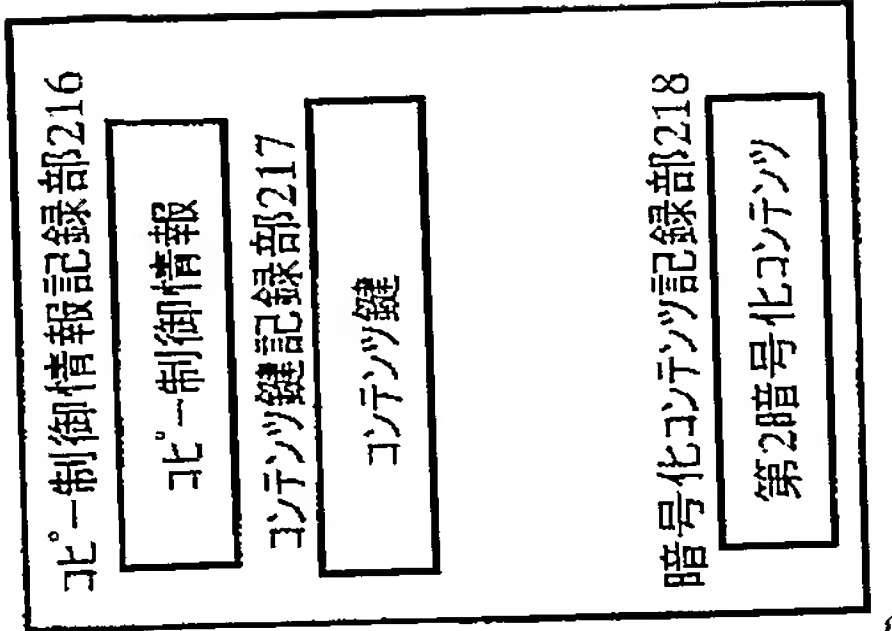
【図 6】

可搬媒体

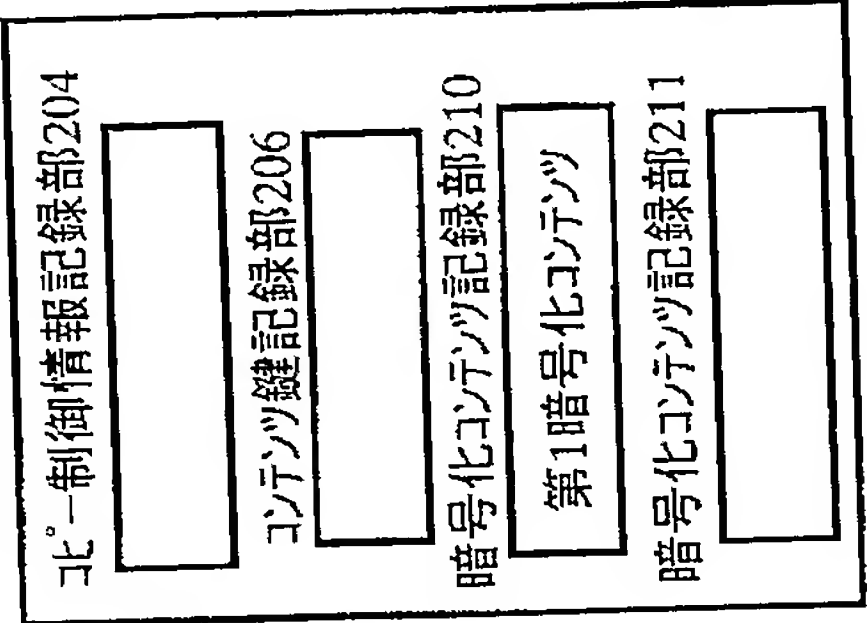
記録再生装置

可搬媒体

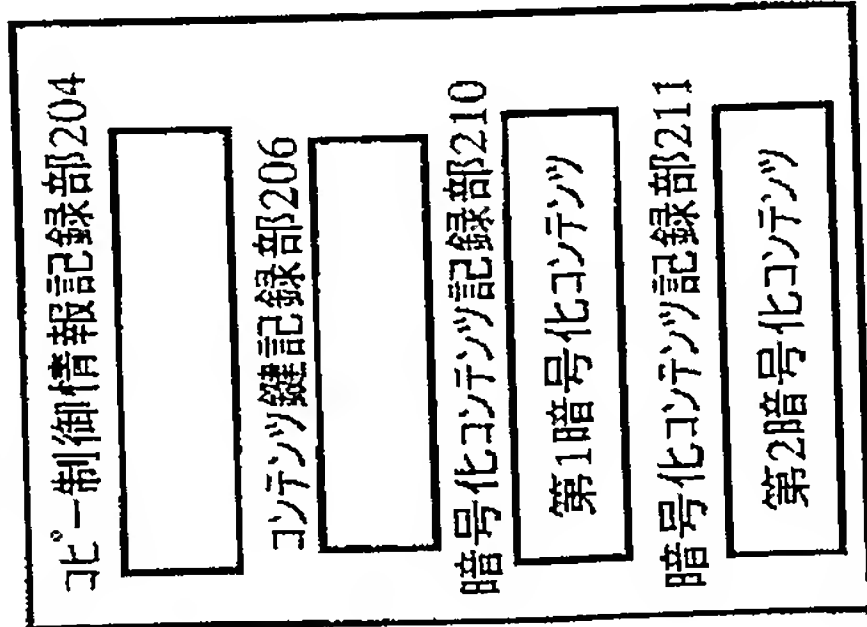
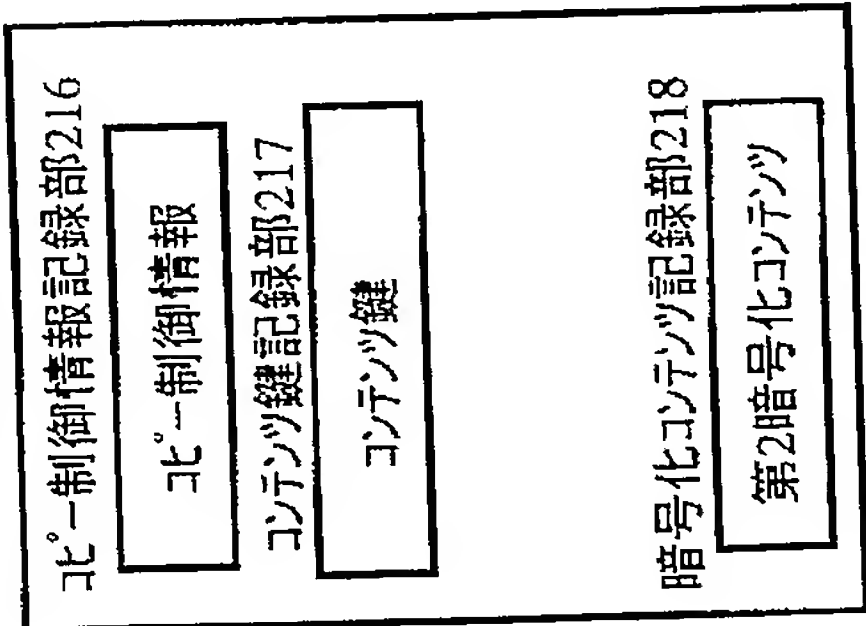
記録再生装置



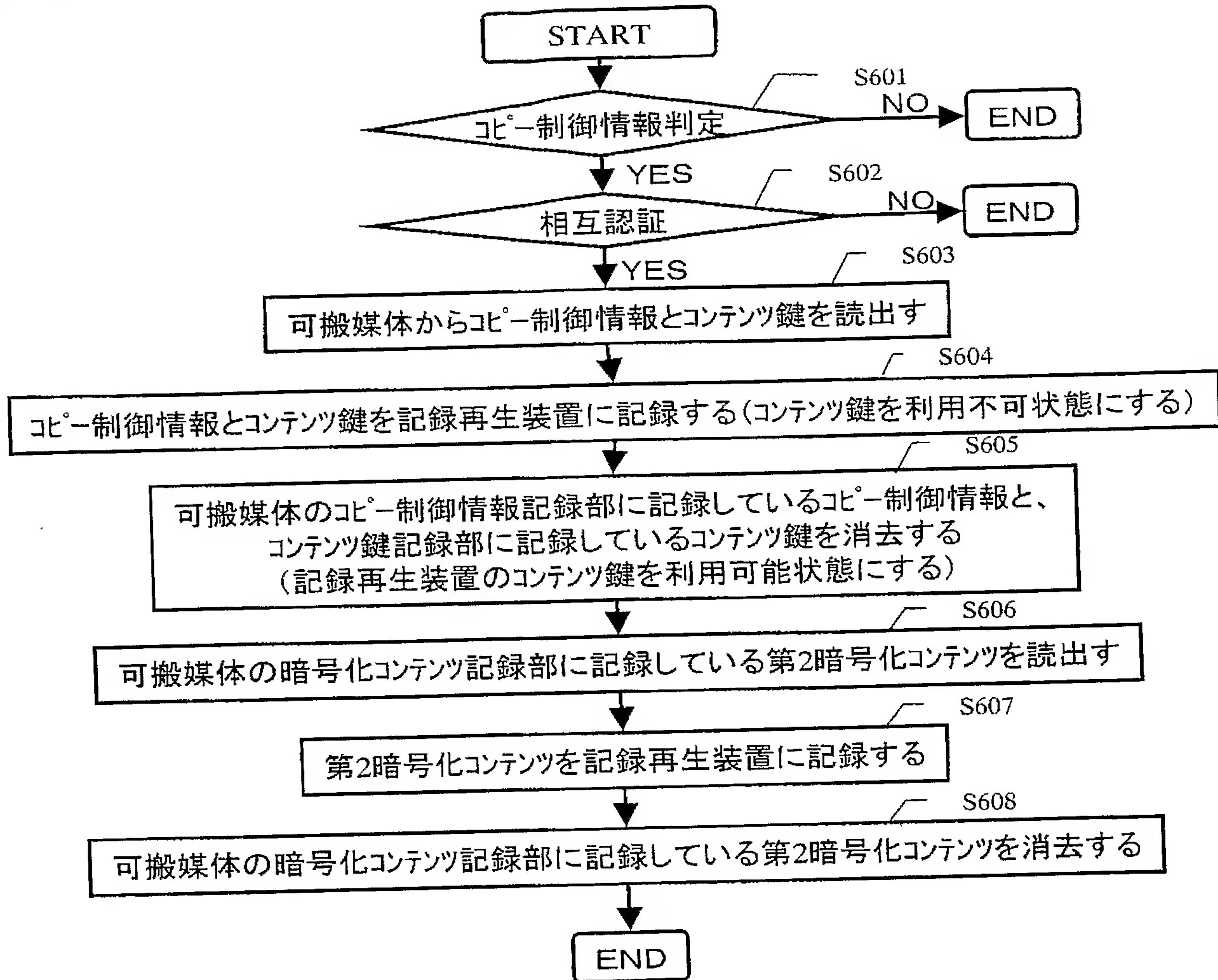
(f)



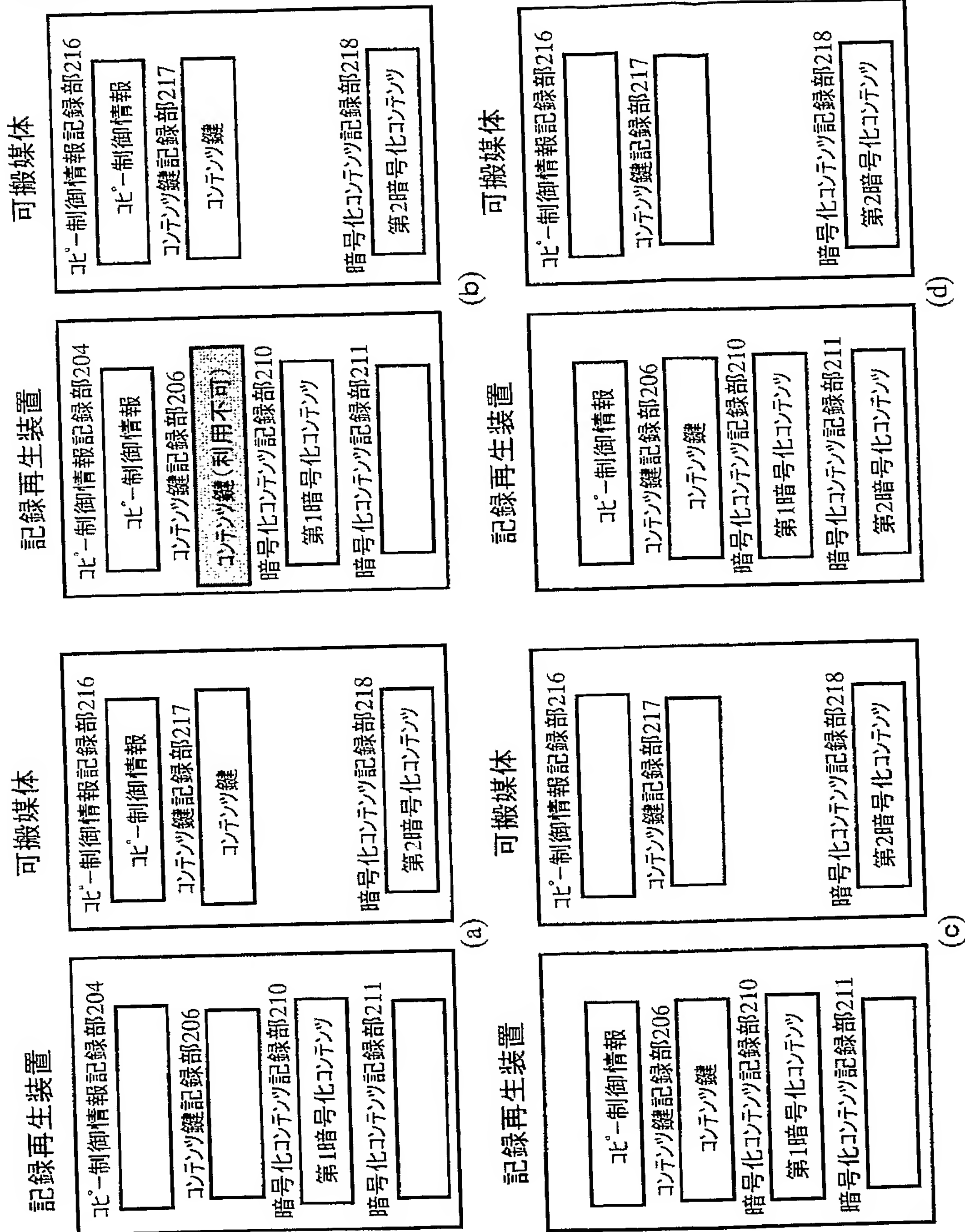
(e)



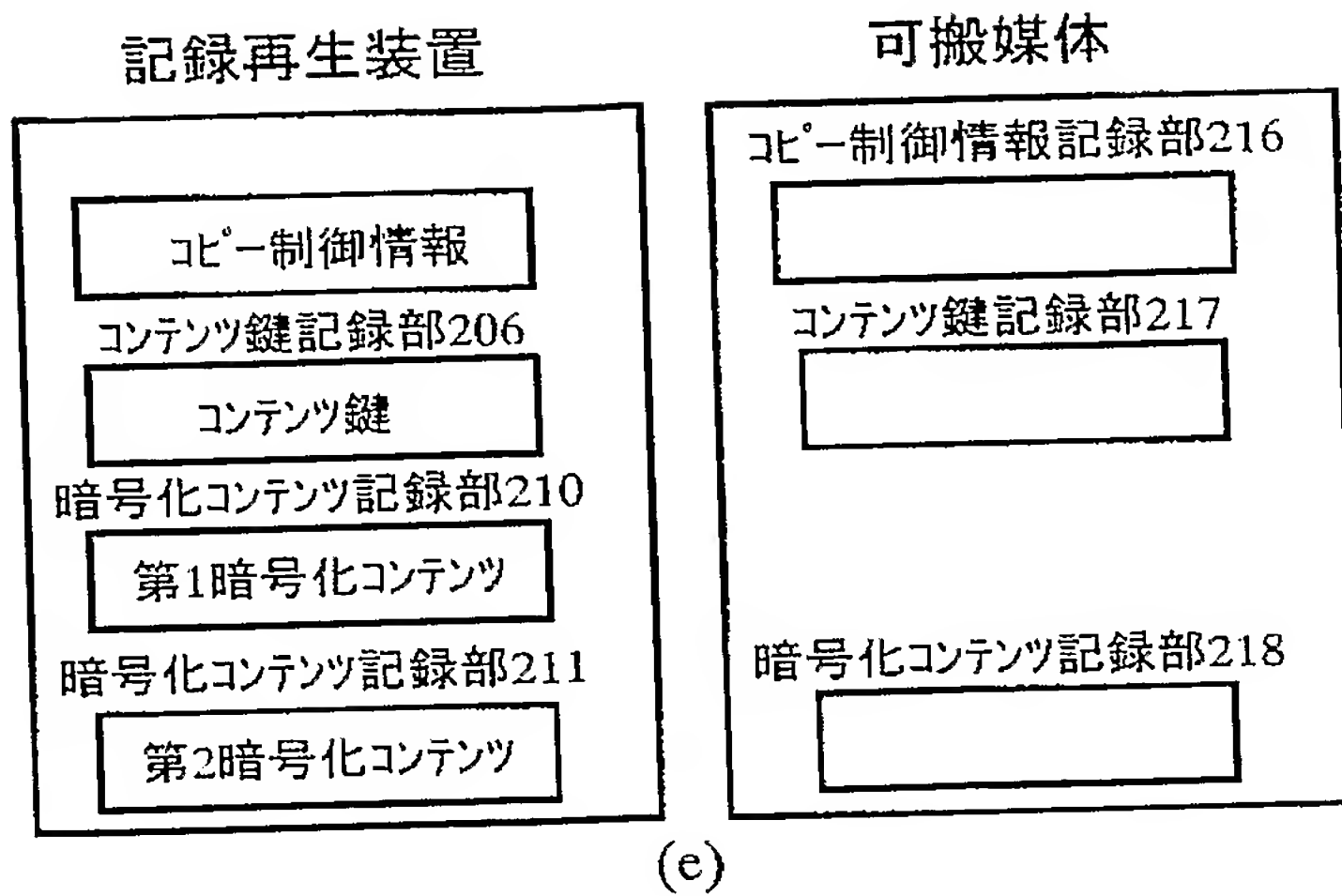
【図 7】



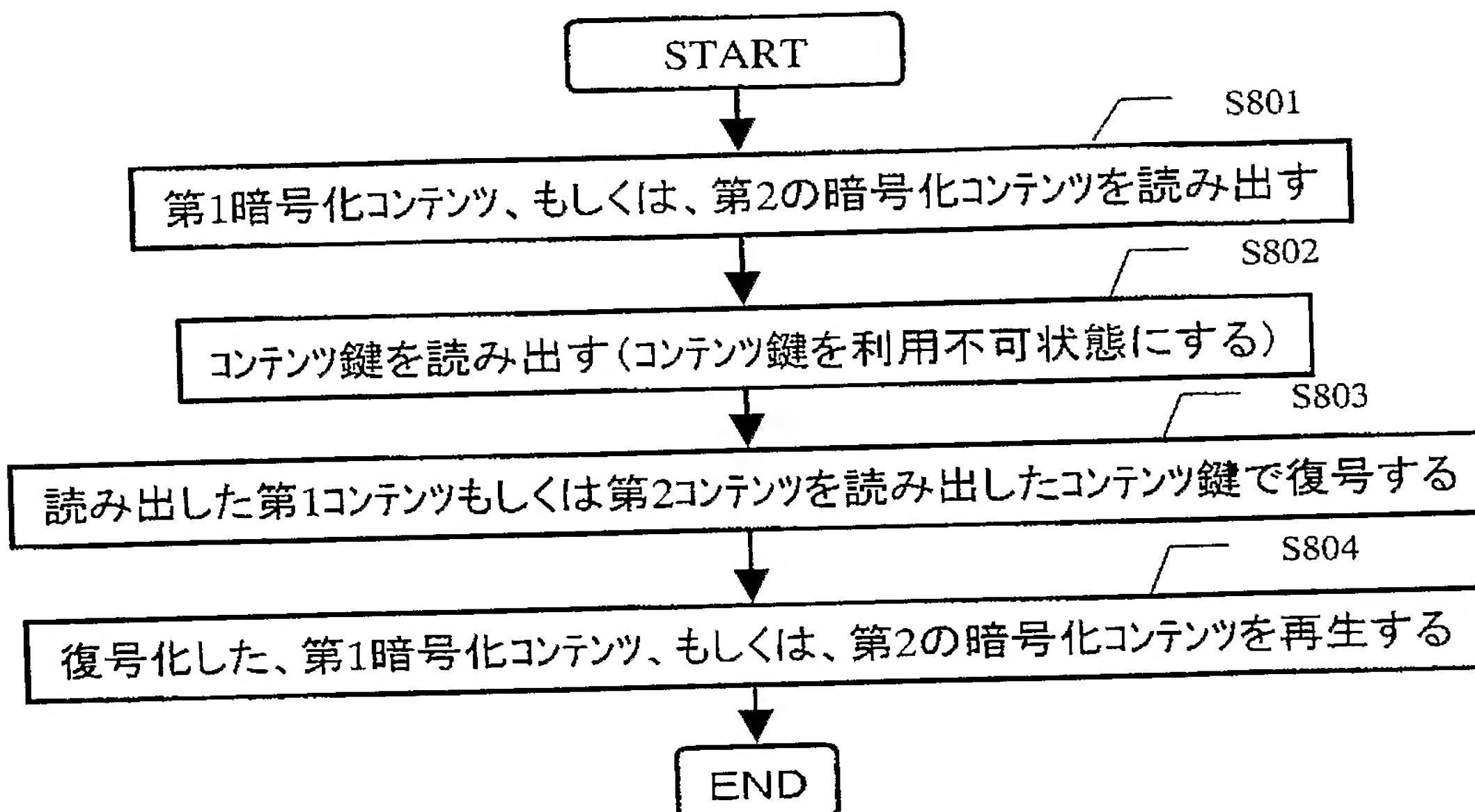
【図 8】



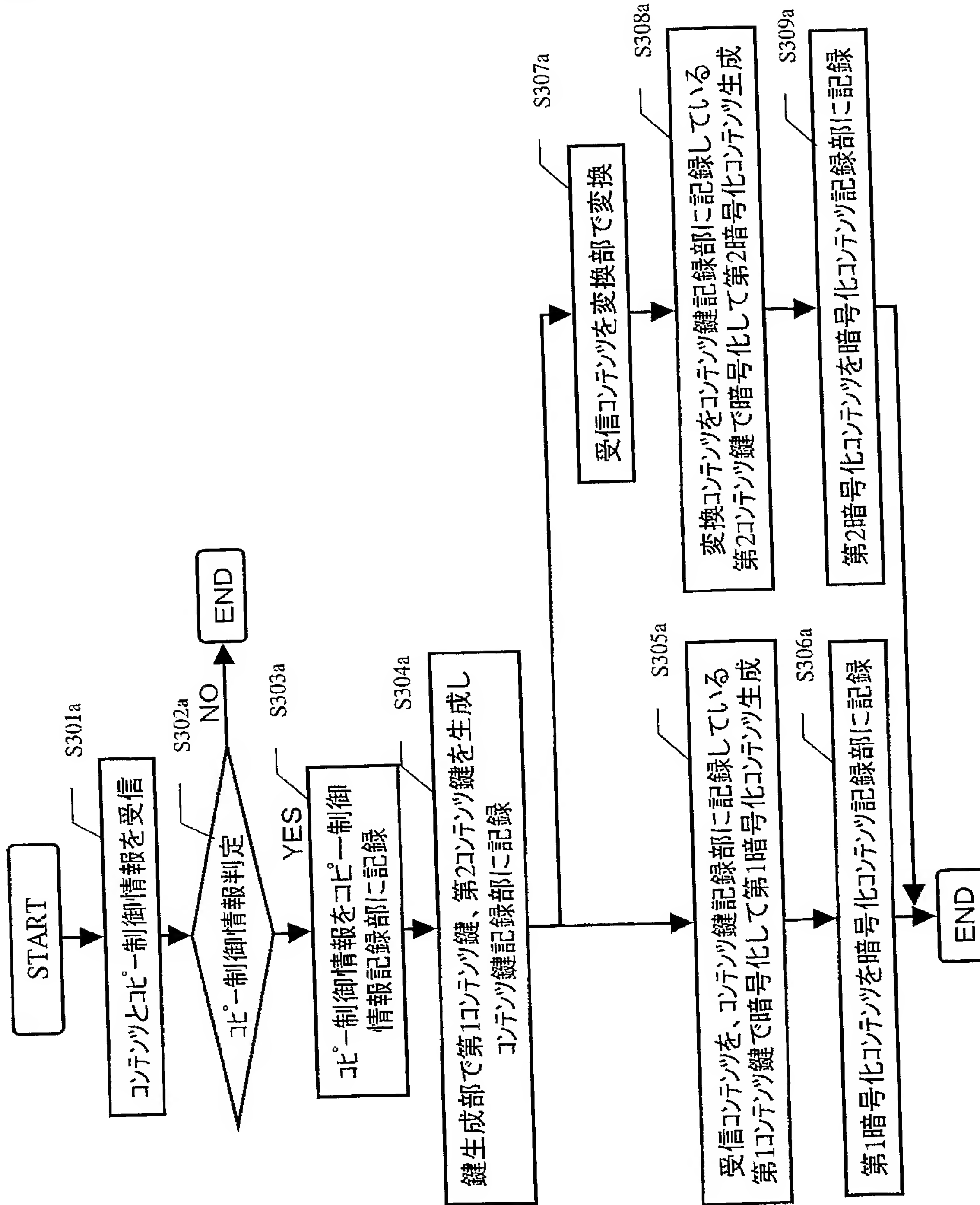
【図 9】



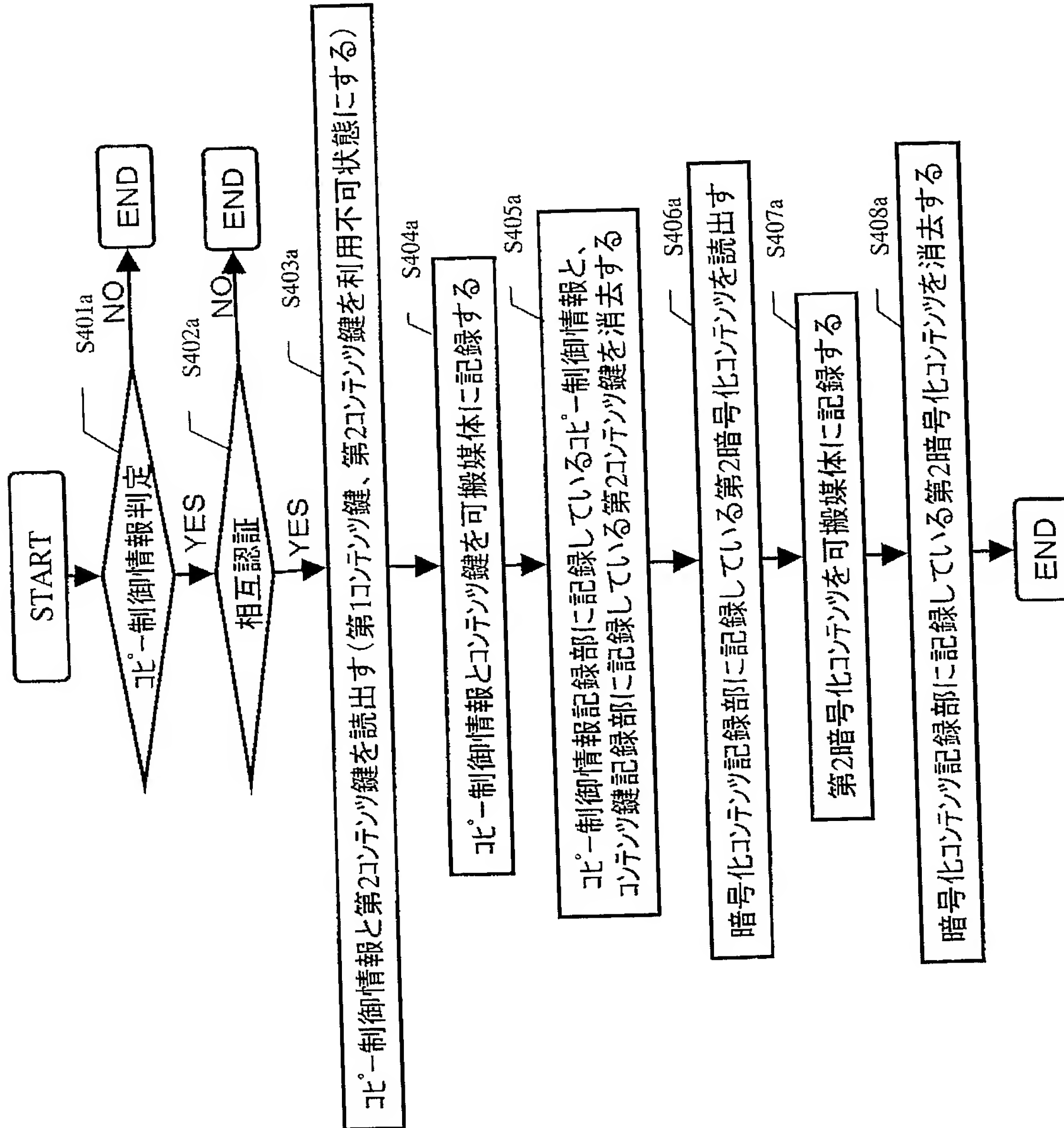
【図 10】



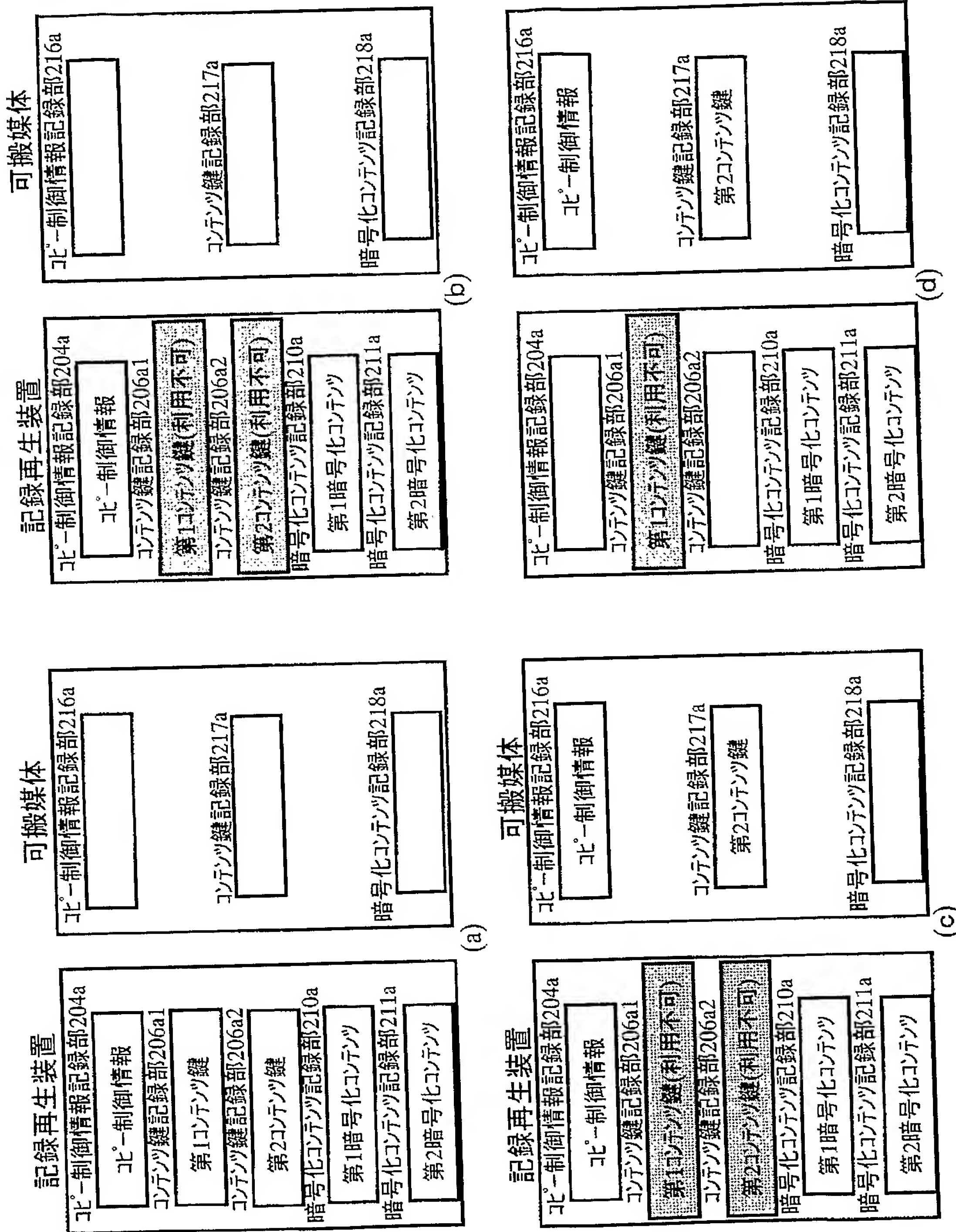
【図 12】



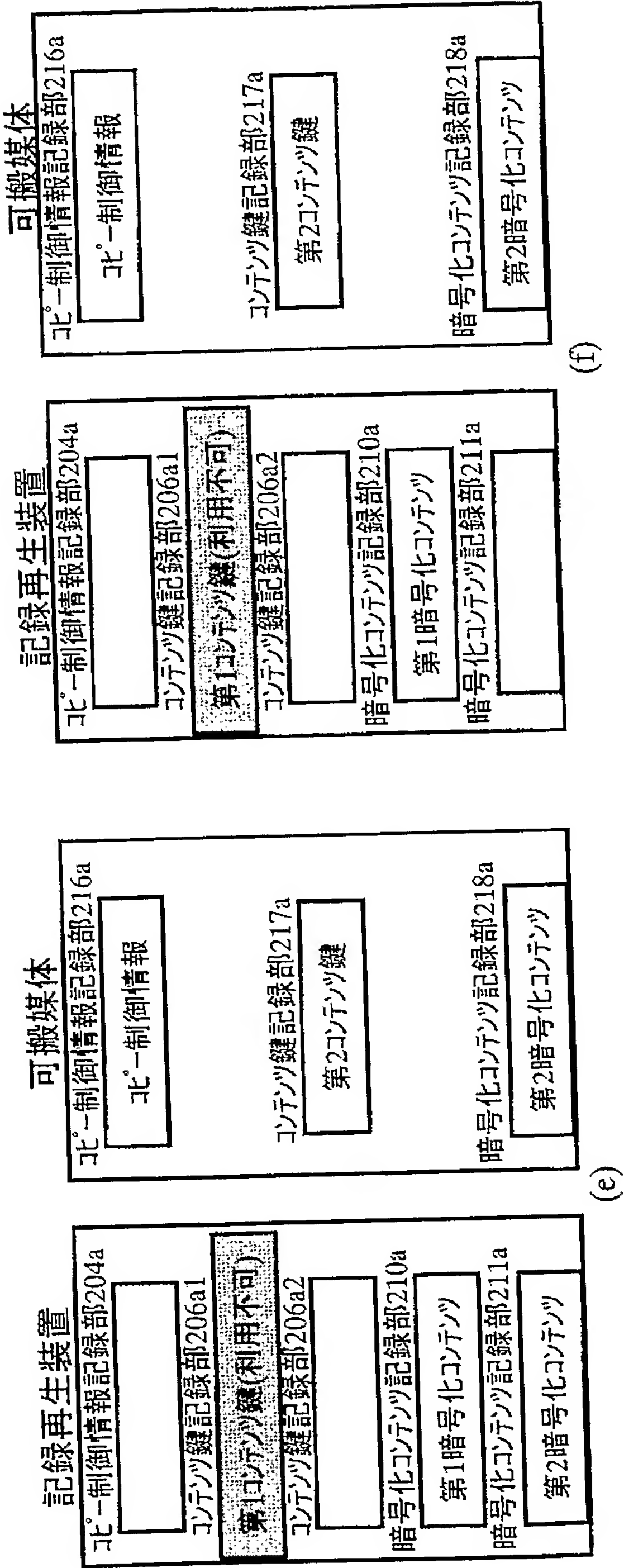
【図 13】



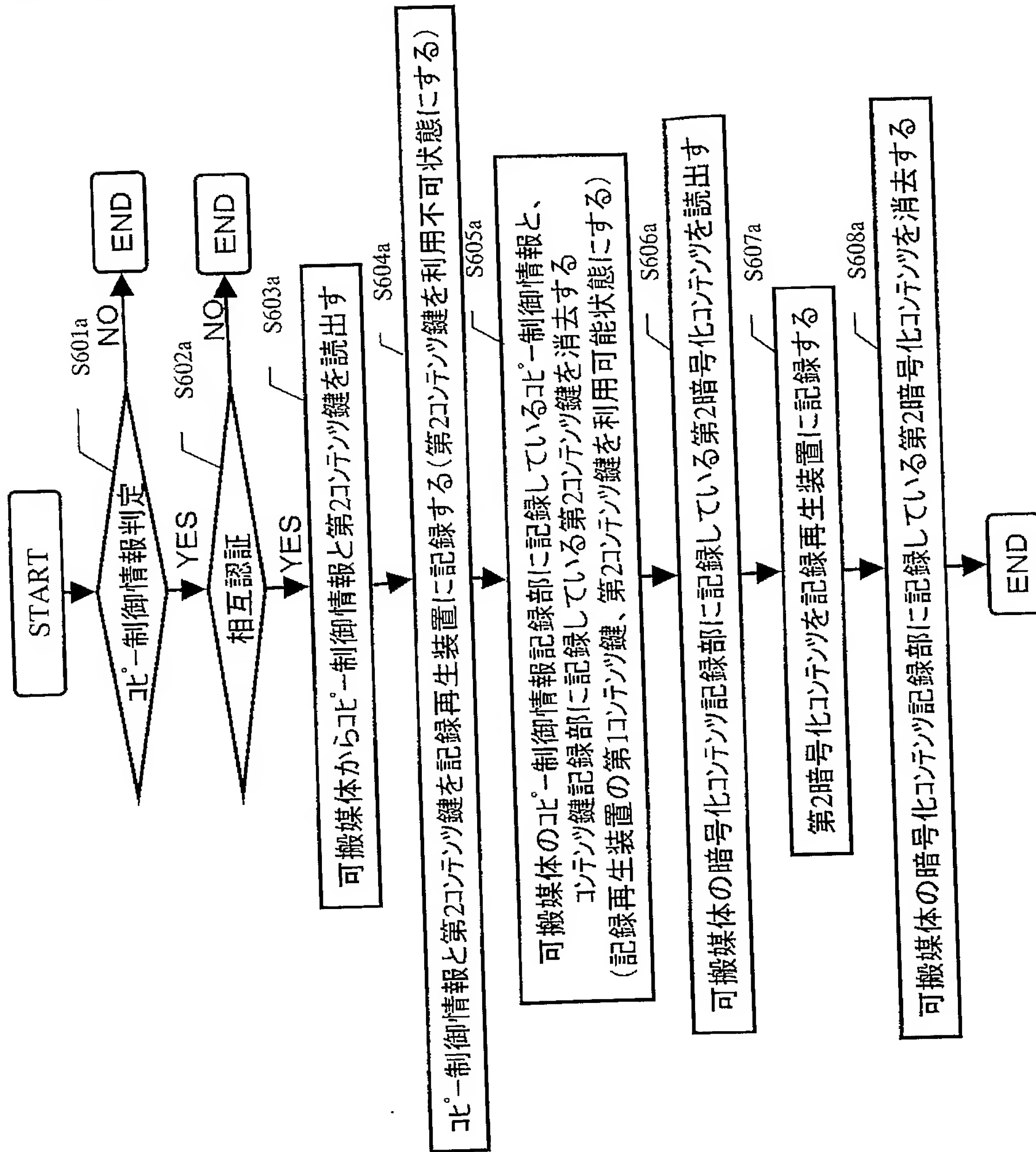
【図 14】



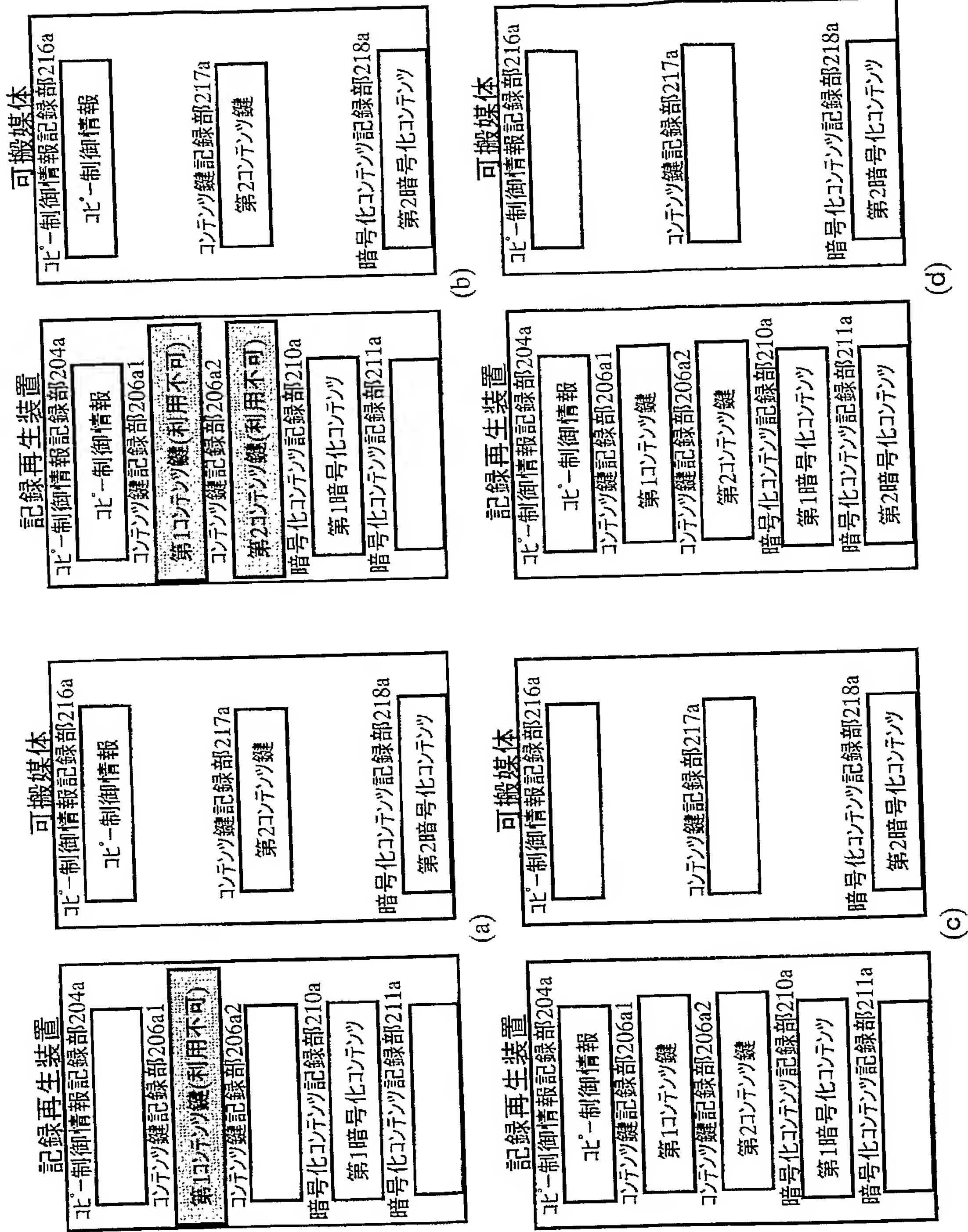
【図 1 5】



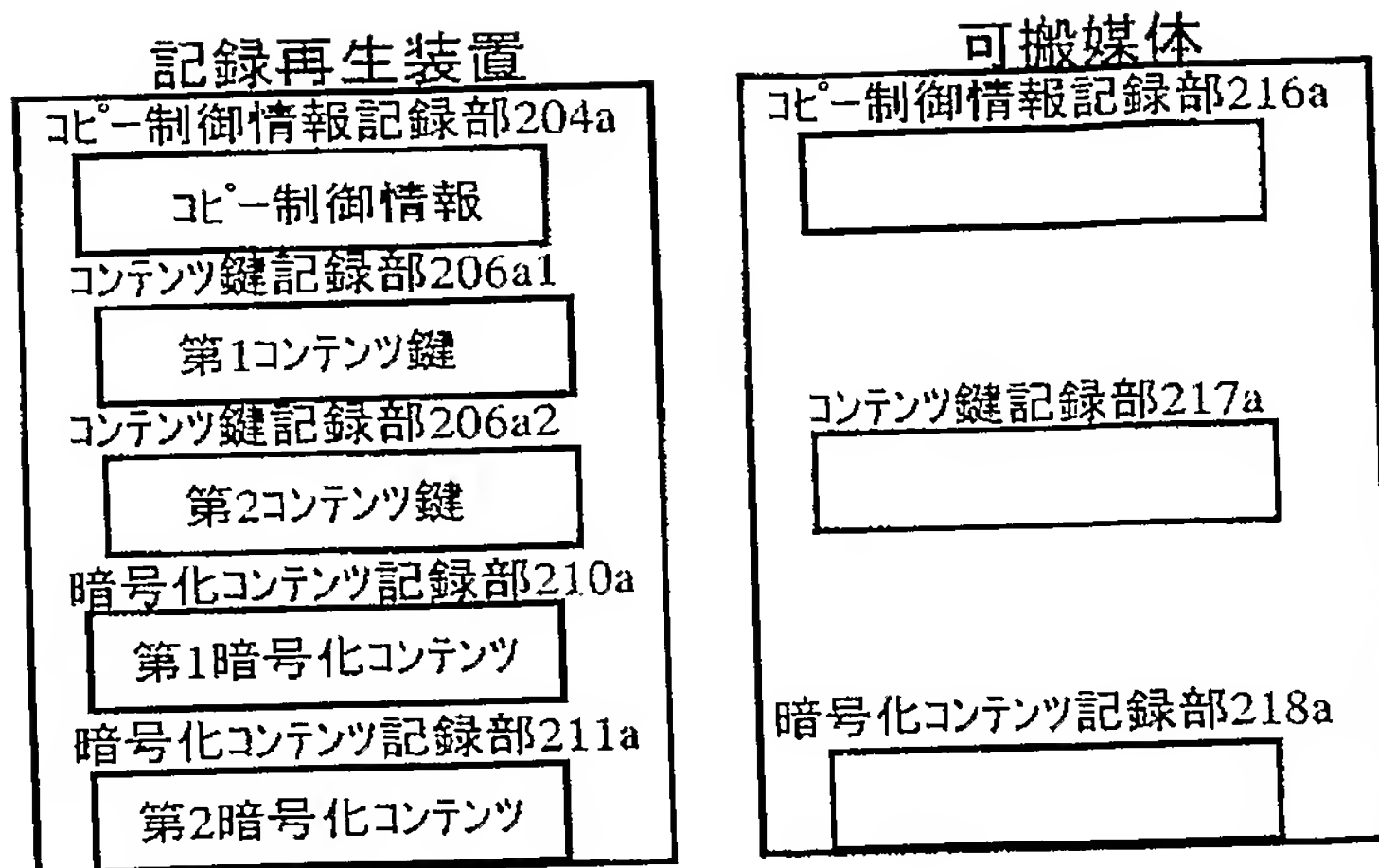
【図 16】



【図 17】

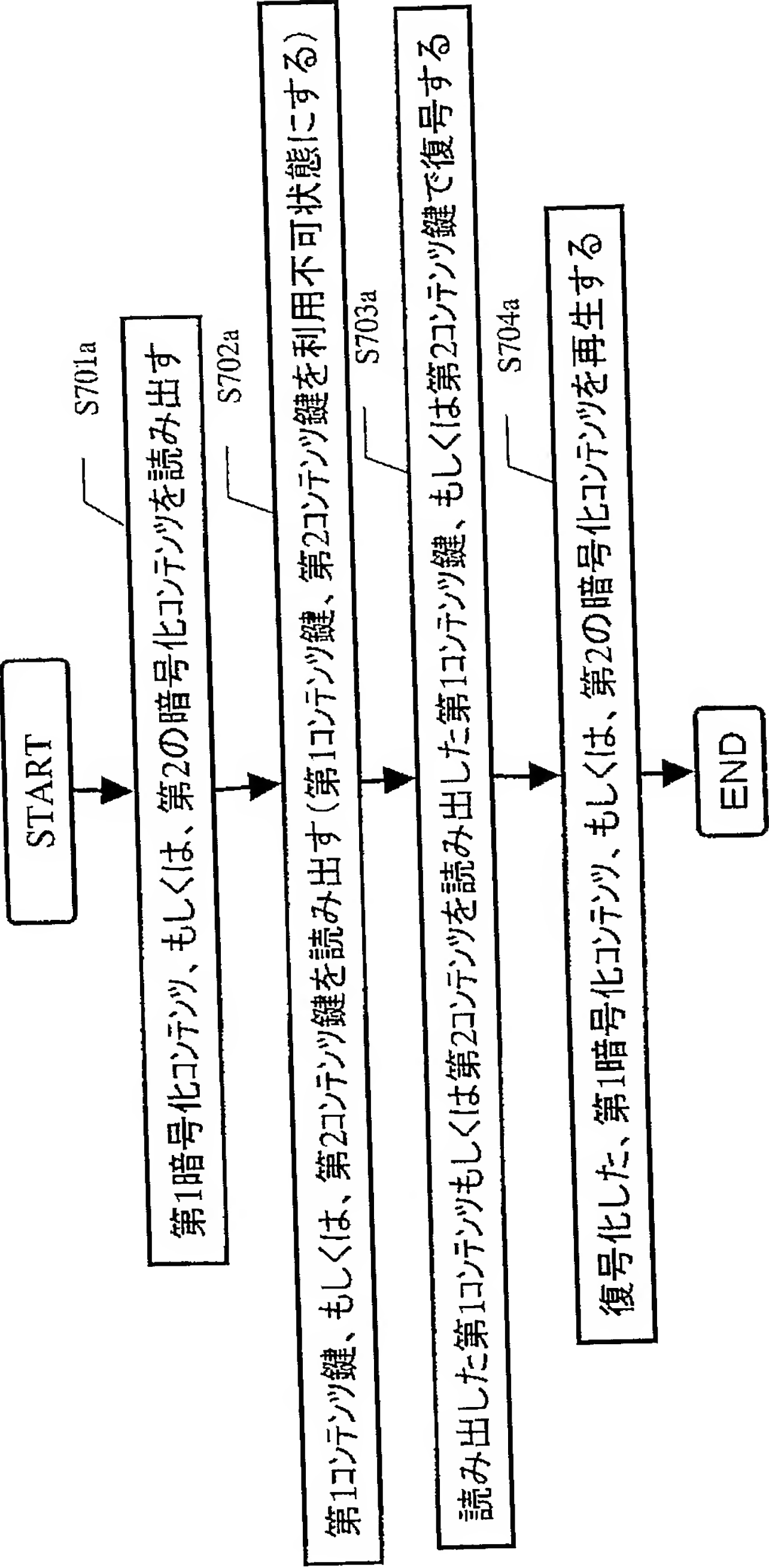


【図 18】



(e)

【図 1 9】



【書類名】 要約書**【要約】**

【課題】 高画質コンテンツの画質を劣化させるなどしてサイズを小さく圧縮変換してからコンテンツの移動を行った場合、圧縮変換されたコンテンツだけが残ってしまう。

【解決手段】 記録再生装置は、高画質コンテンツと圧縮変換したコンテンツを、それぞれ同じコンテンツ鍵で暗号化し暗号化コンテンツ記録部に記録するとともに、コンテンツ鍵をコンテンツ鍵記録部に記録する。記録再生装置から可搬媒体への移動処理時には、コンテンツ鍵記録部に記録したコンテンツ鍵をメモリカードのコンテンツ鍵記録部に記録すると同時に記録再生装置のコンテンツ鍵記録部から消去する。可搬媒体から記録再生装置への移動処理時には、メモリカードのコンテンツ鍵記録部に記録したコンテンツ鍵を、記録再生装置のコンテンツ鍵記録部に記録すると同時に、可搬媒体のコンテンツ鍵記録部から消去する。

【選択図】 図 2

特願 2 0 0 4 - 1 2 5 1 9 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社